Implementing Secure Sockets Layer on iSeries

Presented by Barbara Brown
Alliance Systems & Programming, Inc.

September 28, 2004

Alliance Systems & Programming

Agenda

- SSL Concepts
- Digital Certificate Manager
  - Local Certificate Authority
  - Server Certificates
  - User Certificates
  - Signing Certificates
- Applications supporting SSL
- Tips on using SSL
  - Browsers
  - Firewalls

SSL Concepts

Benefits of SSL :

- Encryption (prevents data from being read in transit)
- Ensure Data Integrity (data not modified in transit)
- Authenticate Server identity
- Authenticate Client identity (SSL V3)

History:

- 1994 - SSL Version 1.0 developed by Netscape and RSA
- 1995 - Netscape and RSA create V2.0 and implement it in their products
- SSL V2.0 became the de facto industry standard widely used today
- V2.0 has some security weaknesses and missing functionality, such as client authentication.
- 1996 - Netscape published SSL V3.0.
- Both V2 and V3 in use today

SSL Concepts

Data encryption and decryption :

- Server sends it's certificate to client
- Optionally, server may request client certificate (SSL V3)
- Client creates secret key, encrypts it with server's public key, and sends encrypted key back.
- Server uses its private key to decrypt the secret key
- From then on, secret key is used (requires less computation that public/private key pairs)
- Secret key automatically expires after a specific time. (24 hours recommended for V3.0)

SSL Concepts

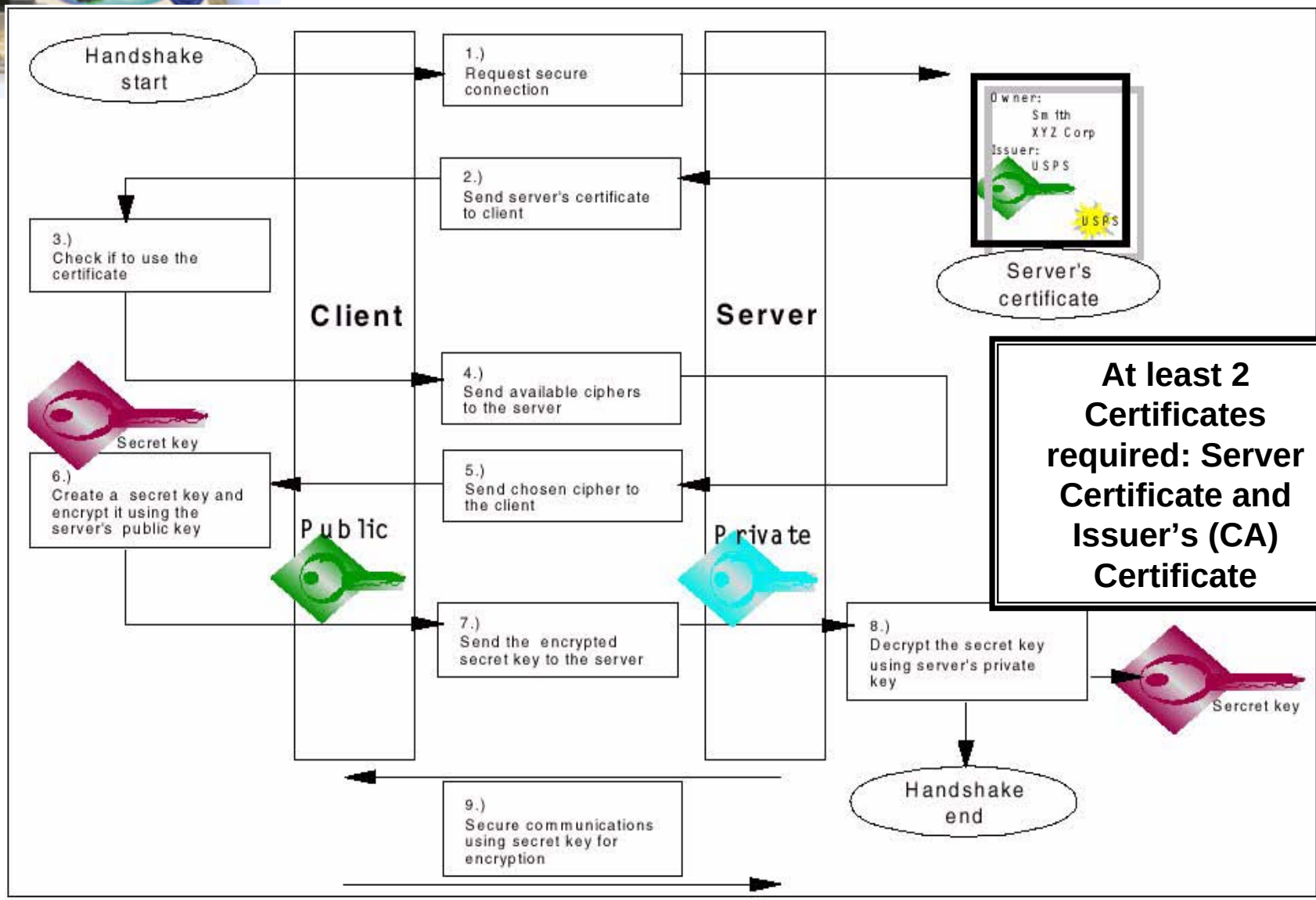
Data integrity

- Message digest (secure hash) built from original data processed with an authentication algorithm
- Hash itself is encrypted and added to sent data.
- Receiver decrypts hash and compares it with newly calculated hash

Authentication

- Optional
- Server certificate used to verify identity
- Certifying authority consulted to confirm
- Client certificate can also be used to verify client identity

SSL Concepts: Handshake



At least 2 Certificates required: Server Certificate and Issuer's (CA) Certificate

SSL Concepts:Handshake

- **Client Hello: client sends request to connect to SSL-enabled server using port number for secure version of the protocol being used.**
- **The server sends back its Server Hello message and its certificate.**
- **The client checks if the certificate was issued by a CA it trusts. If so it checks that the certificate is valid. If either of these checks fails the client can cancel the connection or choose to proceed without authentication.**
- **The client tells the server what ciphers, or types of encryption keys, it can use for communication.**
- **The server chooses the strongest common cipher and informs the client about its selection.**
- **Using that cipher, the client generates a session key (an encryption key to be used only for this session) and encrypts it using the server's public key.**
- **The client sends the encrypted session key to the server.**
- **The server receives the session key and decrypts it using its private key.**
- **This completes the handshake and henceforth the client and server use the session key to encrypt and decrypt the data they send and receive.**

iSeries Requirements for SSL

- **OS/400 V4R1 or higher (some applications must be at higher release levels)**
- **One of the IBM Cryptographic Access Provider products 5722-AC1 (40-bit), 5722-AC2 (56-bit), or 5722-AC3 (128-bit)**
- **Digital Certificate Manager (DCM), option 34 of OS/400 (5722-SS1)**
- **TCP/IP Connectivity Utilities for AS/400 (5722-TC1)**
- **IBM HTTP Server for AS/400 (5722-DG1)**
- **If you want to use SSL with any iseries access component, including iSeries Navigator, you must also install at least one of the AS/400 Client Encryption products: 5722-CE1 (40-bit), 5722-CE2 (56-bit), or 5722-CE3 (128-bit).**
- **Client must also support SSL**

SSL Concepts: Certificate Authority

- **Organization that issues digital certificate**
- **Should have controls to prevent fraud**
- **Internet Certificate Authorities**
  - **National Certificate Authorities: Certiposte, Asociación Nacional de Notariado Mexicano, Deutsche Telekom, Belgacom, ...**
  - **GTE Cybertrust**
  - **Integrion**
  - **RSA**
  - **Thawte**
  - **VeriSign**
    - **and more...**
- **AS/400 can be it's own certificate authority**

SSL Concepts: Which Certificate Authority?

Use an Internet Certificate Authority when...

- You are serving SSL across the Internet
- You are serving SSL to the general public, customers, or business partners that require the assurance of a third party CA
- You are serving SSL to an intranet and do not want to have to train users how to receive your CA certificate into their browsers.
- You do not want to operate your own CA.
- You want to accept certificates that users already have.
- The number of certificates to be issued is large and you do not want the job of having to validate the information people give.

Be your own certificate authority when...

- You want to operate your own CA to control the issuing process.
- You want to identify users in advance.
- Trust is based on organization.

Create a Certificate Authority

IBM®

(C) IBM Corporation 2000

iSeries Tasks

ASPWEB.ALLIANCESYS.COM

http://your400:2001

IBM HTTP Server for iSeries
Configure the iSeries HTTP Server and SSL

Digital Certificate Manager
Create, distribute, and manage Digital Certificates

IBM IPP Server for iSeries
Configure the IBM IPP Server

Related task information

Help
(Requires JavaScript)

Create a Certificate Authority

Digital Certificate Manager - Netscape

File Edit View Go Communicator Help

Back Forward Reload Home Search Netscape Print Security Shop Stop

Bookmarks Location: http://192.168.111.205:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0 What's Related

Instant Message Internet Lookup New&Cool

Digital Certificate Manager IBM

- Certificate Authority (CA)
  - Create a Certificate Authority
- System Certificates
- User Certificates

Return to AS/400 Tasks

Create a Certificate Authority

The system will create a public-private key pair and store the key pair in the def

Key size: 2048 (bits)

Certificate store password: (required)

Confirm password: (required)

Certificate Information

Certificate Authority name: (required)

Organization unit:

Organization name: (require

Locality or city:

State or province: (require

Country: (required)

Validity period of Certificate Authority (1-2000): 1095 (days)

OK Cancel

Document: Done

Each certificate store has it's own password. REMEMBER YOUR PASSWORD!!

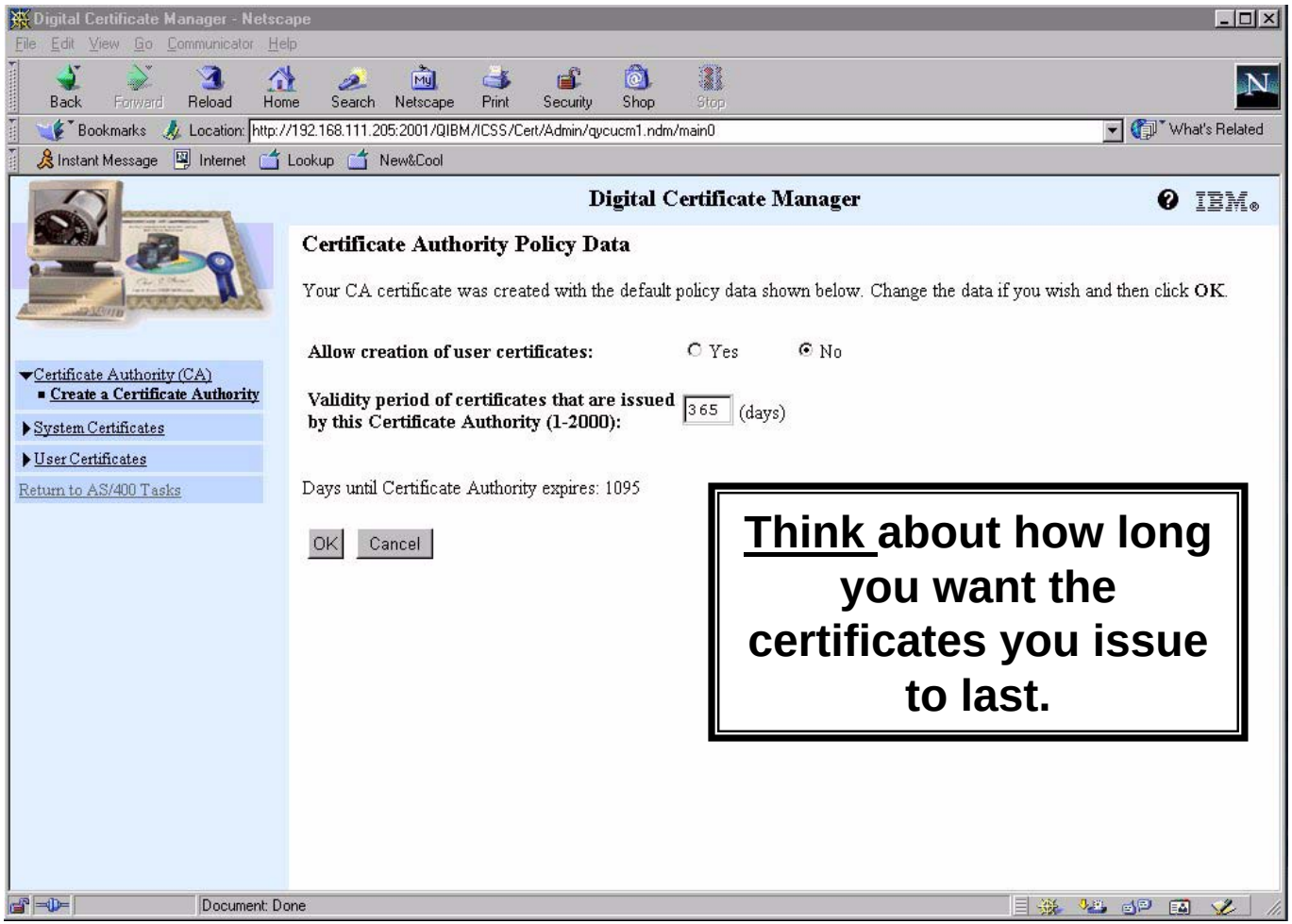
Alas… all certificates expire… NOTE IT ON YOUR CALENDAR a month in advance!

Create a Certificate Authority

Digital Certificate Manager - Netscape
File Edit View Go Communicator Help
Bookmarks Go to: http://your_system_name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
What's Related
Digital Certificate Manager
IBM
CA Certificate Created Successfully
A certificate for your Certificate Authority was created and stored in the default CA certificate store.
Users must install the certificate to make use of the security provided by the certificate.
Certificate Authority (CA)
Create a Certificate Authority
System Certificates
User Certificates
Return to AS/400 Tasks
Click the following link to install the certificate on your browser. Your web browser will display several windows to help you complete the installation of the certificate.
Receive Certificate
You will now provide the policy data to be used for signing and issuing certificates with this Certificate Authority.
OK
Cancel

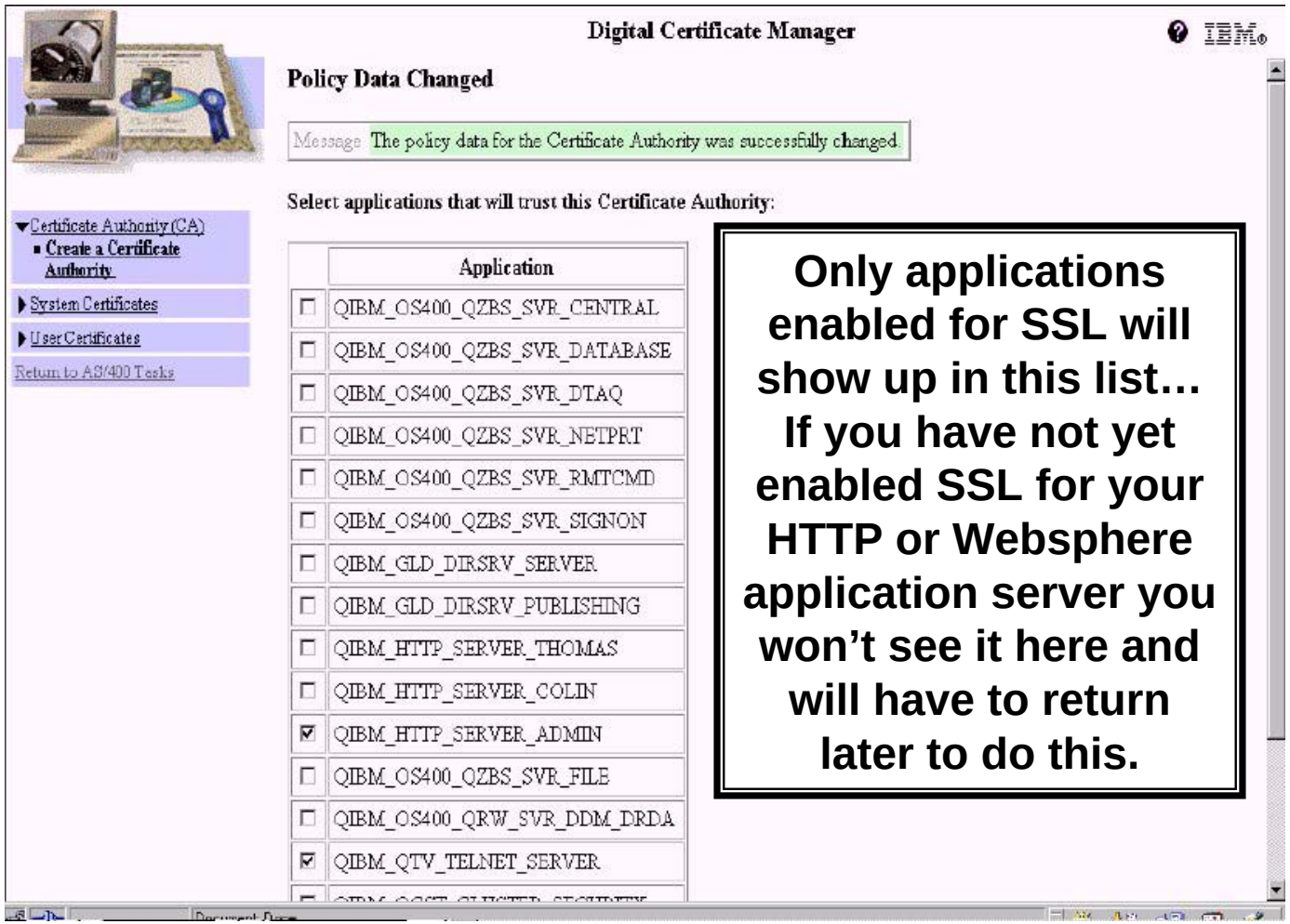
<u>Do</u> receive the certificate and save it on a server somewhere and in your own file system: When using Local CA, you need to import Local CA certificate to the other systems certificate store and set it as trusted

Create a Certifcate Authority

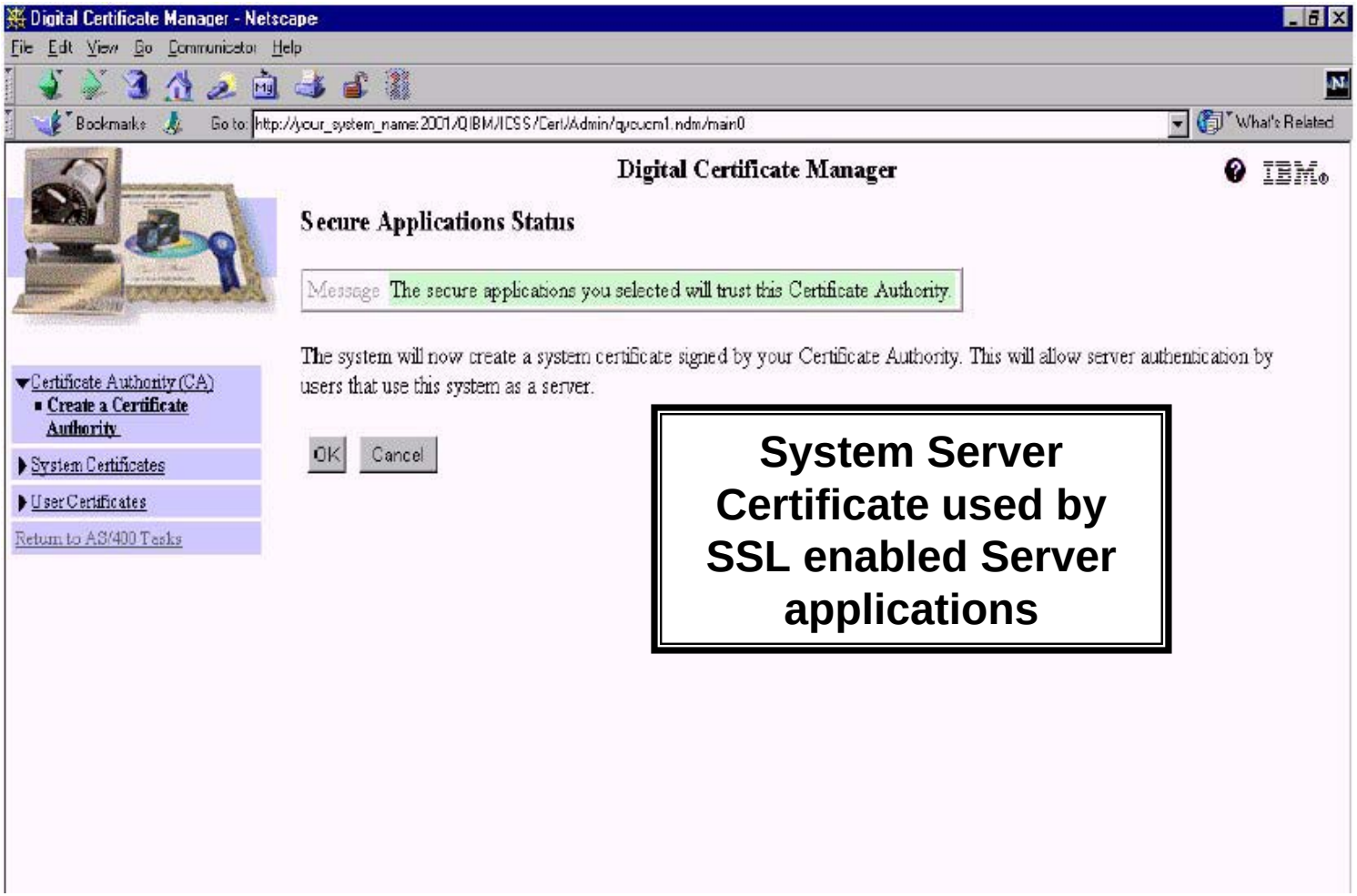

Digital Certificate Manager - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location: http://192.168.111.205:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0 What's Related
Instant Message Internet Lookup New&Cool
Digital Certificate Manager
IBM
Certificate Authority Policy Data
Your CA certificate was created with the default policy data shown below. Change the data if you wish and then click OK.
Allow creation of user certificates: Yes No
Validity period of certificates that are issued by this Certificate Authority (1-2000): 365 (days)
Days until Certificate Authority expires: 1095
OK Cancel
Certificate Authority (CA)
Create a Certificate Authority
System Certificates
User Certificates
Return to AS/400 Tasks
Document: Done

Think about how long you want the certificates you issue to last.

Create a Certifcate Authority



Create a Certifcate Authority


Digital Certificate Manager - Netscape
File Edit View Go Communicator Help
Bookmarks Go to: http://your_system_name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
What's Related
Digital Certificate Manager
IBM
Secure Applications Status
Message The secure applications you selected will trust this Certificate Authority.
The system will now create a system certificate signed by your Certificate Authority. This will allow server authentication by users that use this system as a server.
OK
Cancel
Certificate Authority (CA)
Create a Certificate Authority
System Certificates
User Certificates
Return to AS/400 Tasks

System Server Certificate used by SSL enabled Server applications

Server Certificate

- **Digital ID**
- **Issued by Certifying Authority**
- **Standardized format (X.509 - RFC 2459)**
- **private key of the certificate's public key is held by the entity to whom the certificate was issued and sometimes other trusted parties**
- **A certificate typically holds:**
  - **serial number.**
  - **name of the entity it was created for**
  - **public key of the certificate.**
  - **period for which the certificate is valid.**
  - **name of the CA that issued the certificate**
  - **digital signature from the CA that issued the certificate. (used to prove the validity of the certificate)**

Server Certificates are specific to one server and one name

Create Server Certificate

Digital Certificate Manager - Netscape

File Edit View Go Communicator Help

Bookmarks Go to: http://your_system_name:2001/QIBM/CSS/Cert/Admin/qycucm1.ndm/main0 What's Related

Digital Certificate Manager IBM

- Certificate Authority (CA)
  - Create a Certificate Authority
- System Certificates
- User Certificates

Return to AS/400 Tasks

Create a System Certificate

The system will create a public-private key pair and store the key pair in the default system certificate store.

Key size: 2048 (bits)

Certificate store password: ******** (required)

Confirm password: ******** (required)

Another password to remember.

Certificate Information

Server name: your_system_name (required)

Organization unit: ITSO Raleigh

Organization name: IBM (required)

Locality or city: Cary

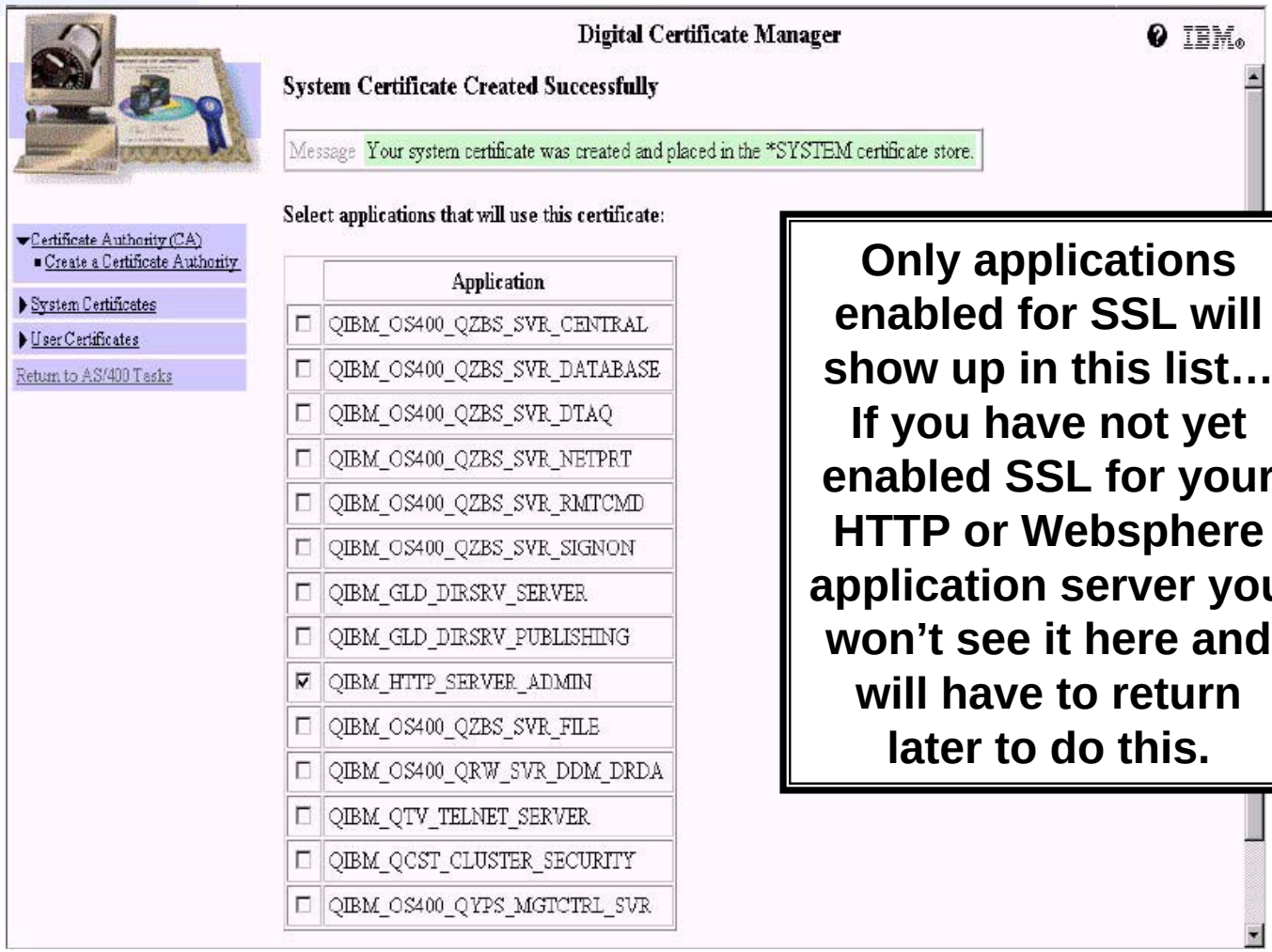
State or province: North Carolina (required minimum of 3 characters)

Country: US (required)

Zip or postal code:

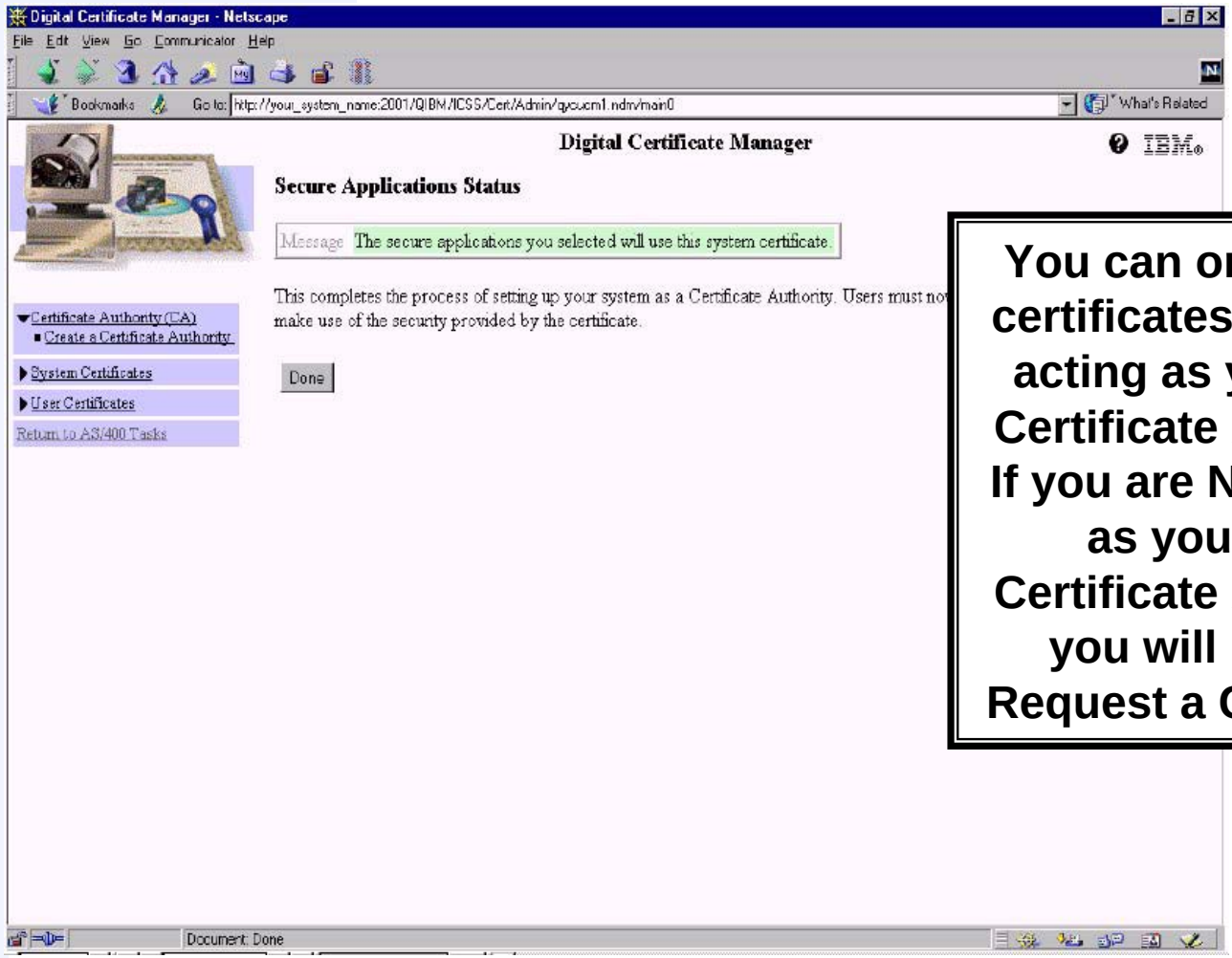
OK Cancel

Create Server Certificate



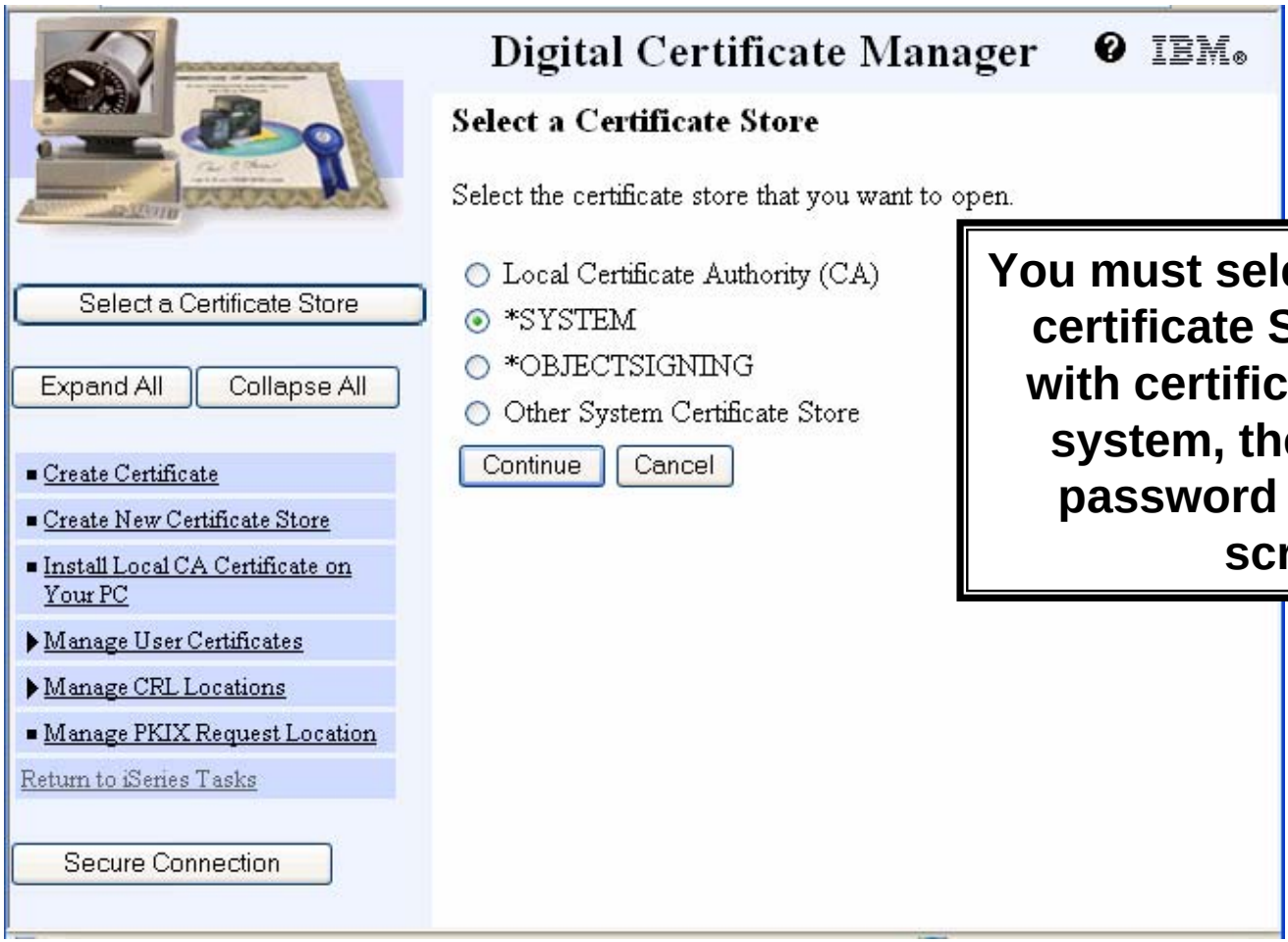
Only applications enabled for SSL will show up in this list… If you have not yet enabled SSL for your HTTP or Websphere application server you won't see it here and will have to return later to do this.

Create Server Certificate


Digital Certificate Manager - Netscape
File Edit View Go Communicator Help
Bookmarks Go to: http://your_system_name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
What's Related
Digital Certificate Manager
IBM
Secure Applications Status
Message The secure applications you selected will use this system certificate.
This completes the process of setting up your system as a Certificate Authority. Users must no
make use of the security provided by the certificate.
Done
Certificate Authority (CA)
Create a Certificate Authority
System Certificates
User Certificates
Return to AS/400 Tasks
Document: Done

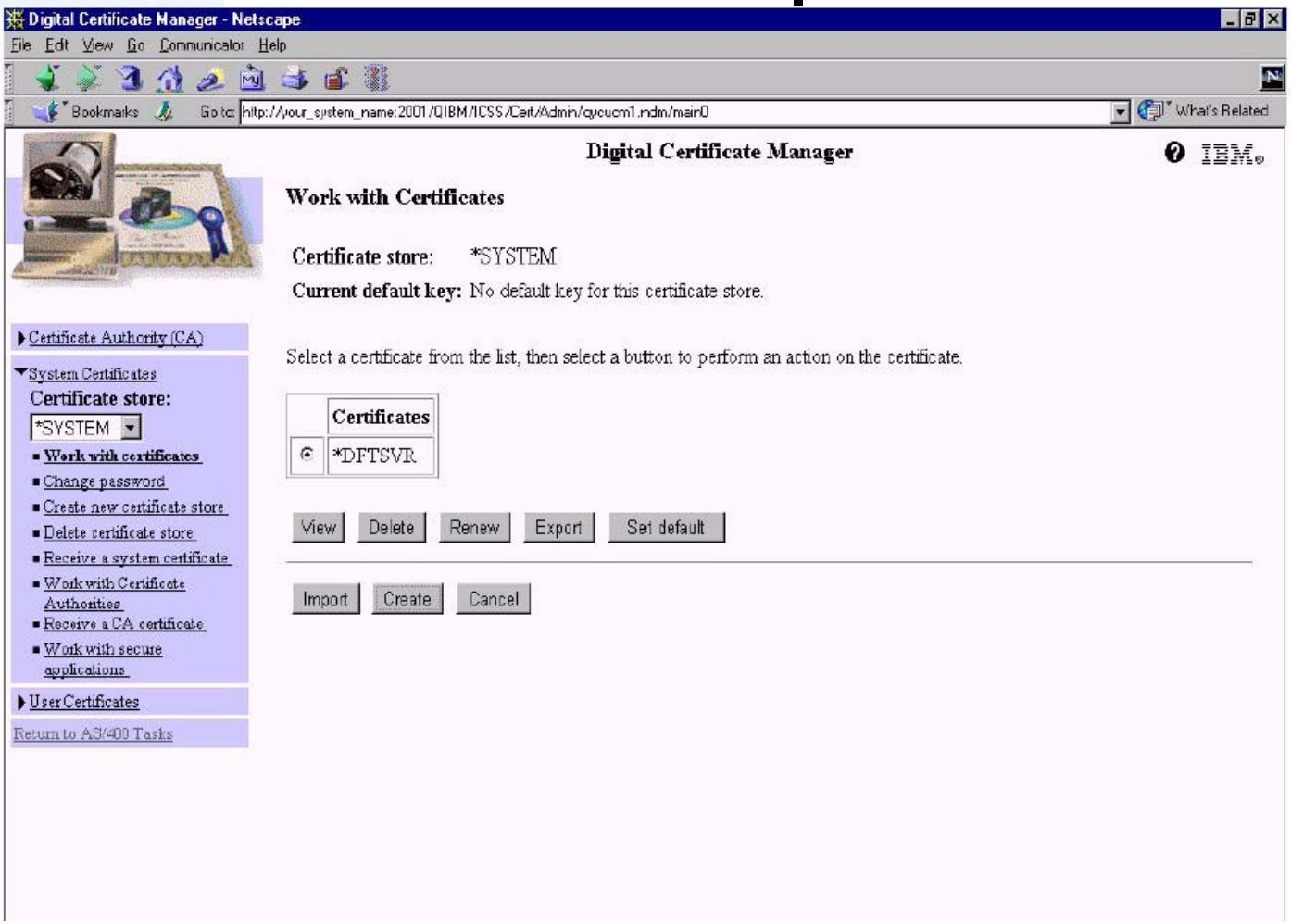
You can only create certificates if you are acting as your own Certificate Authority. If you are NOT acting as your own Certificate Authority, you will need to Request a Certificate.

System Certificate Store



You must select the System certificate Store to work with certificates for your system, then enter the password on the next screen

Create a Certificate Request



Create a Certificate Request

Bookmarks Location: http://your.system.name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0

Digital Certificate Manager

Select a Certificate Authority

Certificate Authority that will sign this certificate:

- ○ Local Certificate Authority
- ◉ VeriSign or other Internet Certificate Authority

OK Cancel

- ▸ Certificate Authority (CA)
- ▾ System Certificates

Certificate store:

*SYSTEM

- **Work with certificates**
- Change password
- Create new certificate store
- Delete certificate store
- Receive a system certificate
- Work with Certificate Authorities
- Receive a CA certificate
- Work with secure applications

- ▸ User Certificates

Return to AS/400 Tasks

Create a Certificate Request

Bookmarks Location: http://your.system.name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0

Digital Certificate Manager

- Certificate Authority (CA)
- System Certificates
  - **Certificate store:** *SYSTEM
  - **Work with certificates**
  - Change password
  - Create new certificate store
  - Delete certificate store
  - Receive a system certificate
  - Work with Certificate Authorities
  - Receive a CA certificate
  - Work with secure applications
- User Certificates

Return to AS/400 Tasks

Create a System Certificate

The system will create a public-private key pair and store the key pair in the certificate store listed below.

Certificate store: *SYSTEM

Key size: 2048 (bits)

Key label: VeriSignServerCertificateTrial (required)

Certificate Information

Server name: www.yourserver.com (required)

Organization unit: ITSO Raleigh

Organization name: IBM (required)

Locality or city: Cary

State or province: North Carolina (required:minimum of 3 characters)

Country: US (required)

Zip or postal code:

OK Cancel

Create a Certificate Request

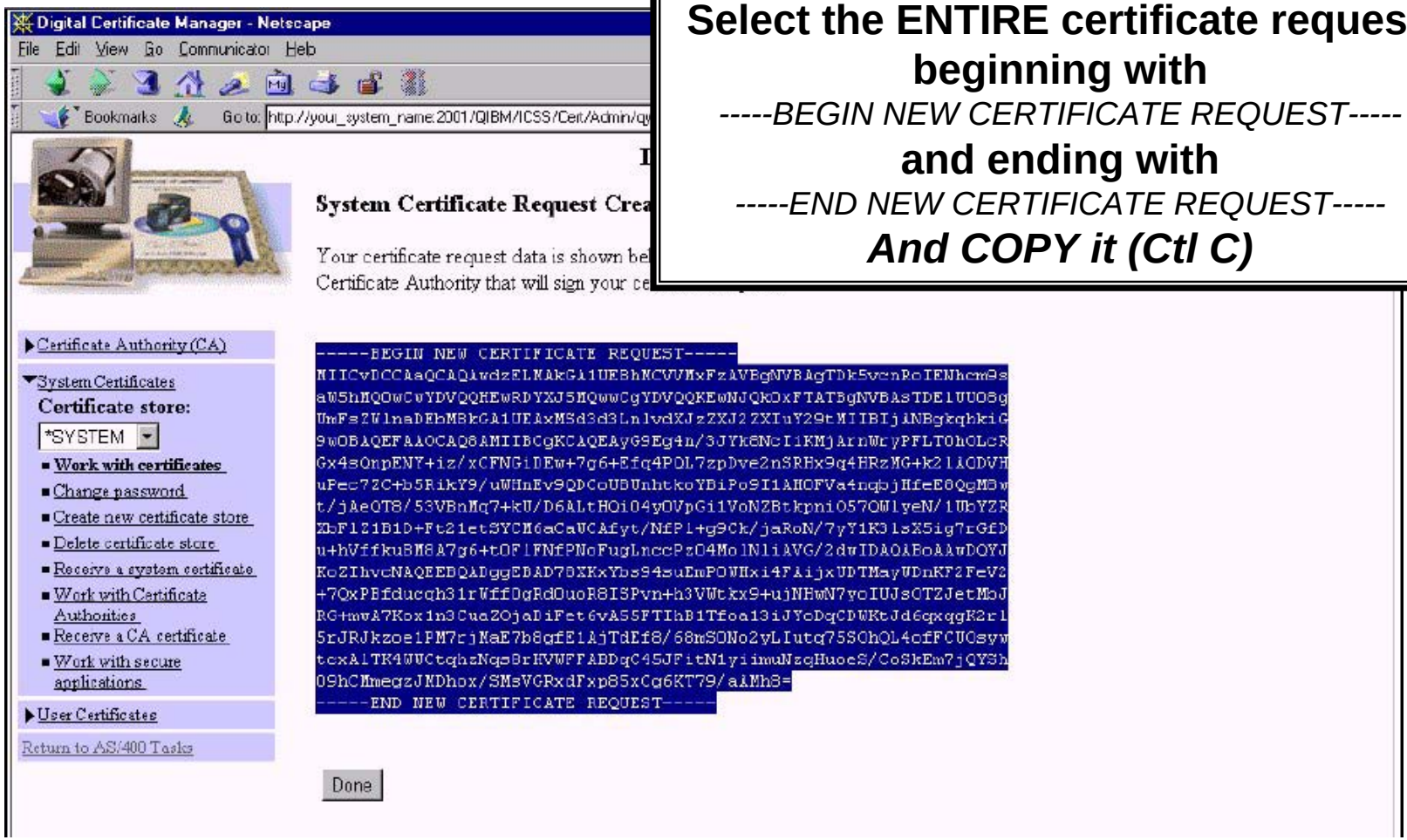
Select the ENTIRE certificate request, beginning with

-----BEGIN NEW CERTIFICATE REQUEST-----

and ending with

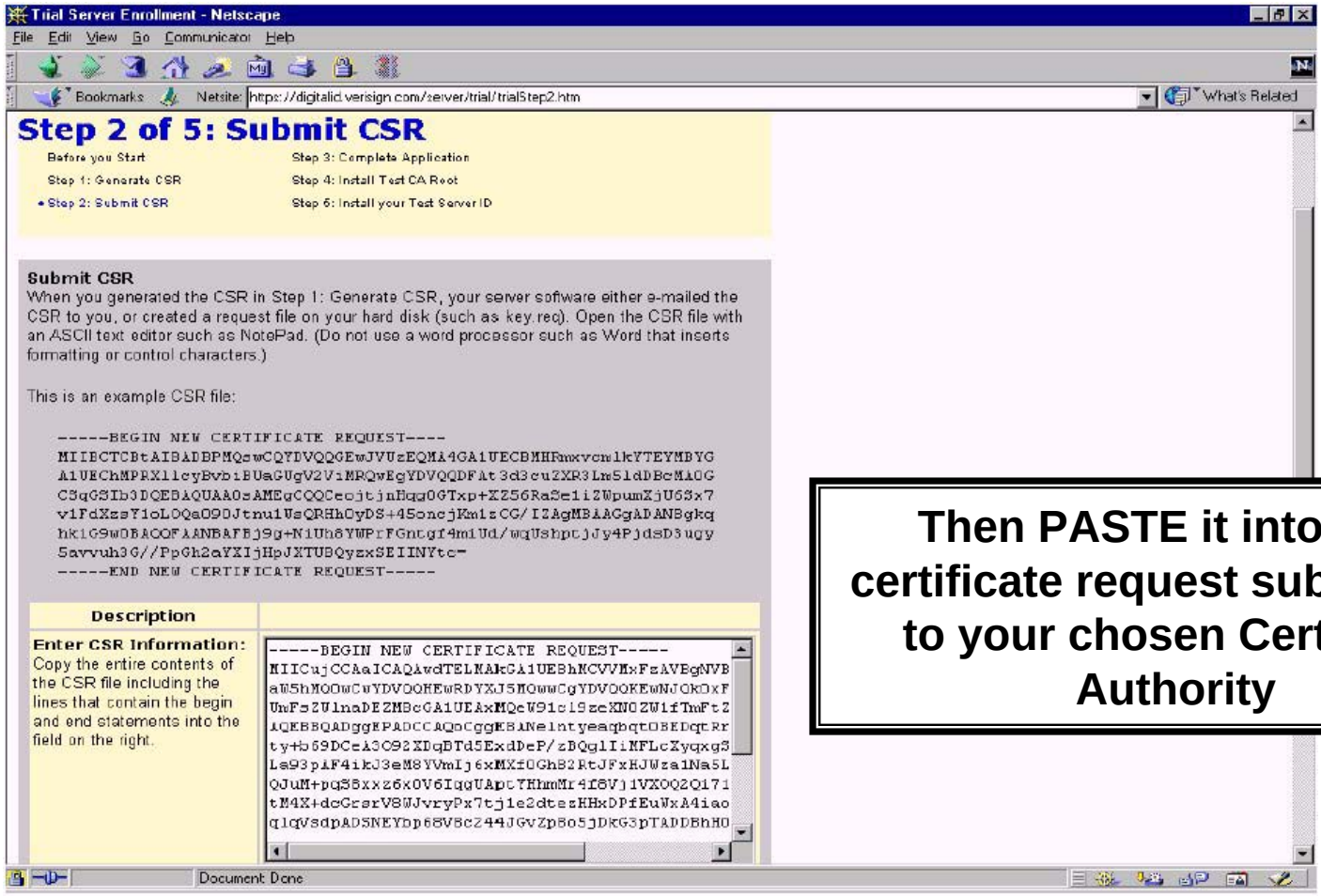
-----END NEW CERTIFICATE REQUEST-----

And COPY it (Ctl C)



Alliance Systems & Programming

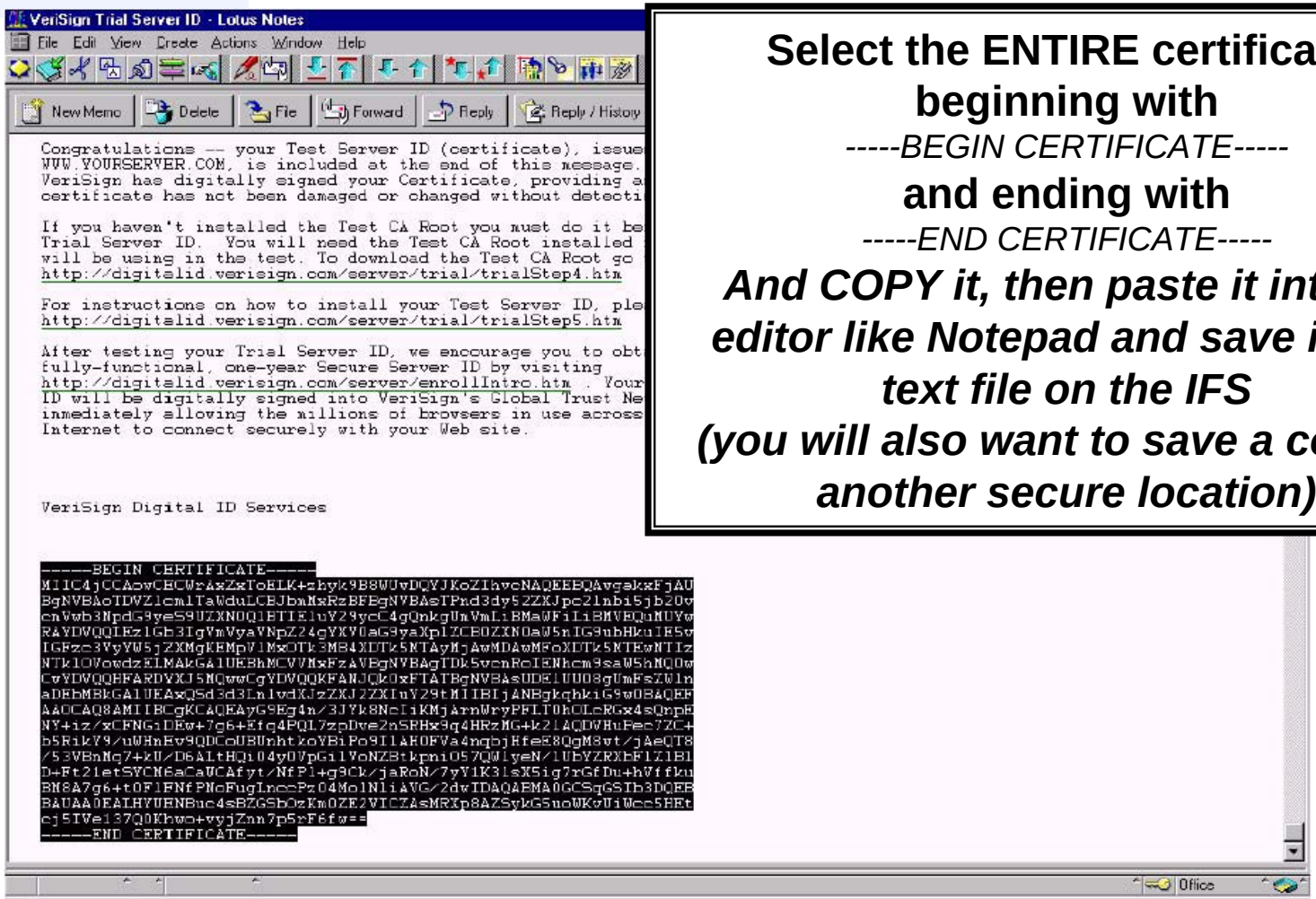
Create a Certificate Request


Trial Server Enrollment - Netscape
File Edit View Go Communicator Help
Bookmarks Netsite: https://digitalid.verisign.com/server/trial/trial5tep2.htm
What's Related
Step 2 of 5: Submit CSR
Before you Start
Step 1: Generate CSR
• Step 2: Submit CSR
Step 3: Complete Application
Step 4: Install Test CA Root
Step 5: Install your Test Server ID
Submit CSR
When you generated the CSR in Step 1: Generate CSR, your server software either e-mailed the CSR to you, or created a request file on your hard disk (such as key.req). Open the CSR file with an ASCII text editor such as NotePad. (Do not use a word processor such as Word that inserts formatting or control characters.)
This is an example CSR file:
-----BEGIN NEW CERTIFICATE REQUEST----
MIIBCTCBtAIBADBPMQswCQYDVQQGEwJVUzEQMA4GA1UECBMHRmxvcmlkYTEYMBYG
A1UEChMPRXllcyBvbiBUaGUgV2ViMRQwEgYDVQQDFAt3d3cuZXR3Lm5ldDBcMA0G
CSqGSIb3DQEBAQUAA0sAMEgCQQCeojtjnHqq0GTxp+ZZ56Ra2e1iZWpumXjU63x7
v1FdXzsY1oLOQaO9DJtnu1VsQRHhOyDS+45oncjKm1zCG/IZAgMBAAGgADANBgkq
hkiG9w0BAQQFAANBAFBj9g+N1Uh8YWPrFGntgf4m1Ud/wqUshpcjJy4PjdsD3ugy
5avvuh3G//PpGh2aYXIjHpJXTUBQyzxSEIINYtc=
-----END NEW CERTIFICATE REQUEST-----
Description
Enter CSR Information:
Copy the entire contents of the CSR file including the lines that contain the begin and end statements into the field on the right.
-----BEGIN NEW CERTIFICATE REQUEST-----
MIICujCCAaICAQAwdTELMAkGA1UEBhMCVVMxFzAVBgNVB
aW5hMOOwCwYDVOOHEwRDYXJ5MOwwCgYDVOOKEwNJOkOxF
UmFsZUlnaDEZMBcGA1UEAxMQeW91cl9zcXNOZW1fTmFtZ
AQEBBQADggEPADCCAQoCggEBANe1ntyeaqbqtOBEDqtRr
ty+b59DCeA3O92XDqBTd5ExdDeP/zBQglIiNFLcZyqxg3
Le93piF4ikJ3eM8YVmIj6xMXfOGhB2RtJFxHJWza1Na5L
QJuM+pq38xxz6x0V6IqqUApcYHhmMr4f8Vj1VXOQ2Q171
tM4X+dcGrsrV8WJvryPx7tj1e2dtesHHxDPfEuWxA4iao
qlqVsdpADSNEYbp68VBcZ44JGvZp5o5jDkG3pTADDBhHO
Document Done

Then PASTE it into your certificate request submission to your chosen Certifying Authority

Alliance Systems & Programming

Receive Certificate from Issuer


VeriSign Trial Server ID - Lotus Notes
File Edit View Create Actions Window Help
New Memo Delete File Forward Reply Reply / History
Congratulations -- your Test Server ID (certificate), issue
WWW.YOURSERVER.COM, is included at the end of this message.
VeriSign has digitally signed your Certificate, providing a
certificate has not been damaged or changed without detecti
If you haven't installed the Test CA Root you must do it be
Trial Server ID. You will need the Test CA Root installed
will be using in the test. To download the Test CA Root go
http://digitalid.verisign.com/server/trial/trialStep4.htm
For instructions on how to install your Test Server ID, ple
http://digitalid.verisign.com/server/trial/trialStep5.htm
After testing your Trial Server ID, we encourage you to obt
fully-functional, one-year Secure Server ID by visiting
http://digitalid.verisign.com/server/enrollIntro.htm . Your
ID will be digitally signed into VeriSign's Global Trust Ne
immediately allowing the millions of browsers in use across
Internet to connect securely with your Web site.
VeriSign Digital ID Services
-----BEGIN CERTIFICATE-----
MIIC4jCCAowCBCWrAxZxToELK+zhyk9B8WUwDQYJKoZIhvcNAQEEBQAwgakxFjAU
BgNVBAoTDVZlcmlTaWduLCBJbmMxRzBFBgNVBAsTPnd3dy52ZXJpc2lnbi5jb20v
cnVwb3NpdG9yeS9UZXNOQ1BTIEluY29ycC4gQnkgUnVmLiBMaWFiLiBMVEQuNUYw
RAYDVQQLEz1Gb3IgVmVyaVNpZ24gYXV0aG9yaXplZCBOZXN0aW5nIG9nbHku1E5v
IGBzc3VyVW5jZXMgKHMpVlMxOTk3MB4XDTk5NTAyMjAwMDAwMFoXDTk5NTEwNTIz
NTk1OVowdzELMAkGA1UEBhMCVVMxFzAVBgNVBAgTDk5vcnRoIENhcm9saW5hNQ0w
CwYDVQQHEARDYXJ5MQwwCgYDVQQKFANJQk0xFTATBgNVBAsUDELUU08gUmFsZW1n
aDEbMBkGA1UEAxQ5d3d3LnlwdXJzZXJ2ZXIuY29tMIIBIjANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEAyG9Eg4n/3IYk8NeIiKMjArnWryPFLT0hOLcRGx4sQnpH
NY+iz/xCFNGiDEw+7g6+Efq4PQL7zpDve2nSRHx9q4HRzMG+k2lAQDVHuPec7ZC+
b5RikY9/uWHnEv9QDCoUBUnhtxoYBiPo9IlAHOFVa4nqbjHfeE8QgM8vt/jAeQT8
/53VBnNq7+kU/D6AltHQi04yOVpG1lVoNZBtkpn1O57QWlyeN/1UbYZRXbF1Z1Bl
D+Ft21etSYCN6aCaUCAfyt/NfPl+g8Ck/jaRoN/7yY1K3lsX5ig7rGfDu+hVffku
BN8A7g6+t0F1FNfPNoFugInccPz04Mo1NliAVG/2dvIDAQABMA0GCSqGSIb3DQEB
BAUAA0EAIHYUENBuc4sBZGSbOzKm0ZE2VICZAsMRXp8AZSykG5uoWKvUiWcc5HEt
cj5IVe137Q0Khwo+vyjZnn7p5rF6fw==
-----END CERTIFICATE-----
Office

Select the ENTIRE certificate, beginning with

-----BEGIN CERTIFICATE-----

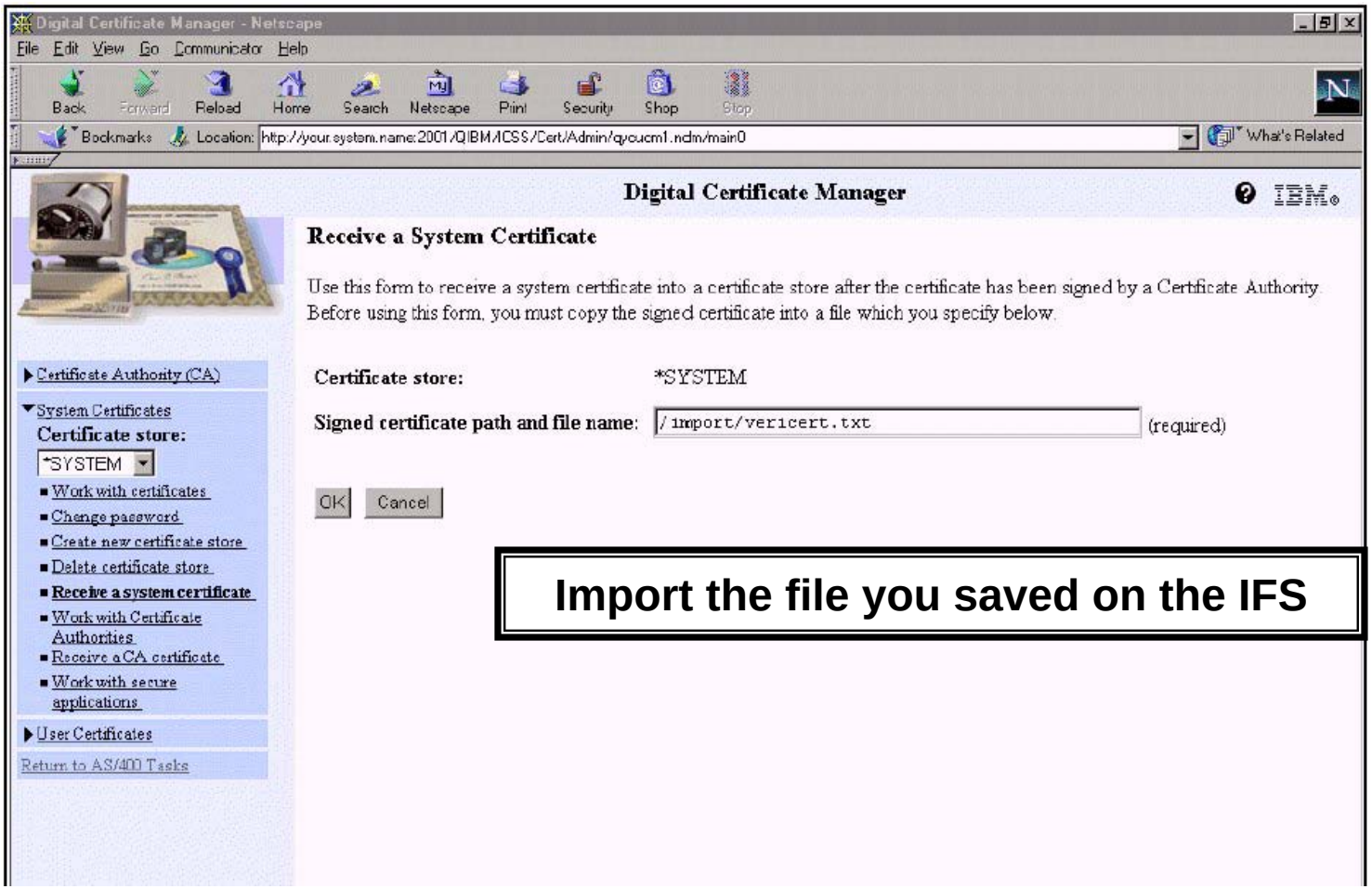
and ending with

-----END CERTIFICATE-----

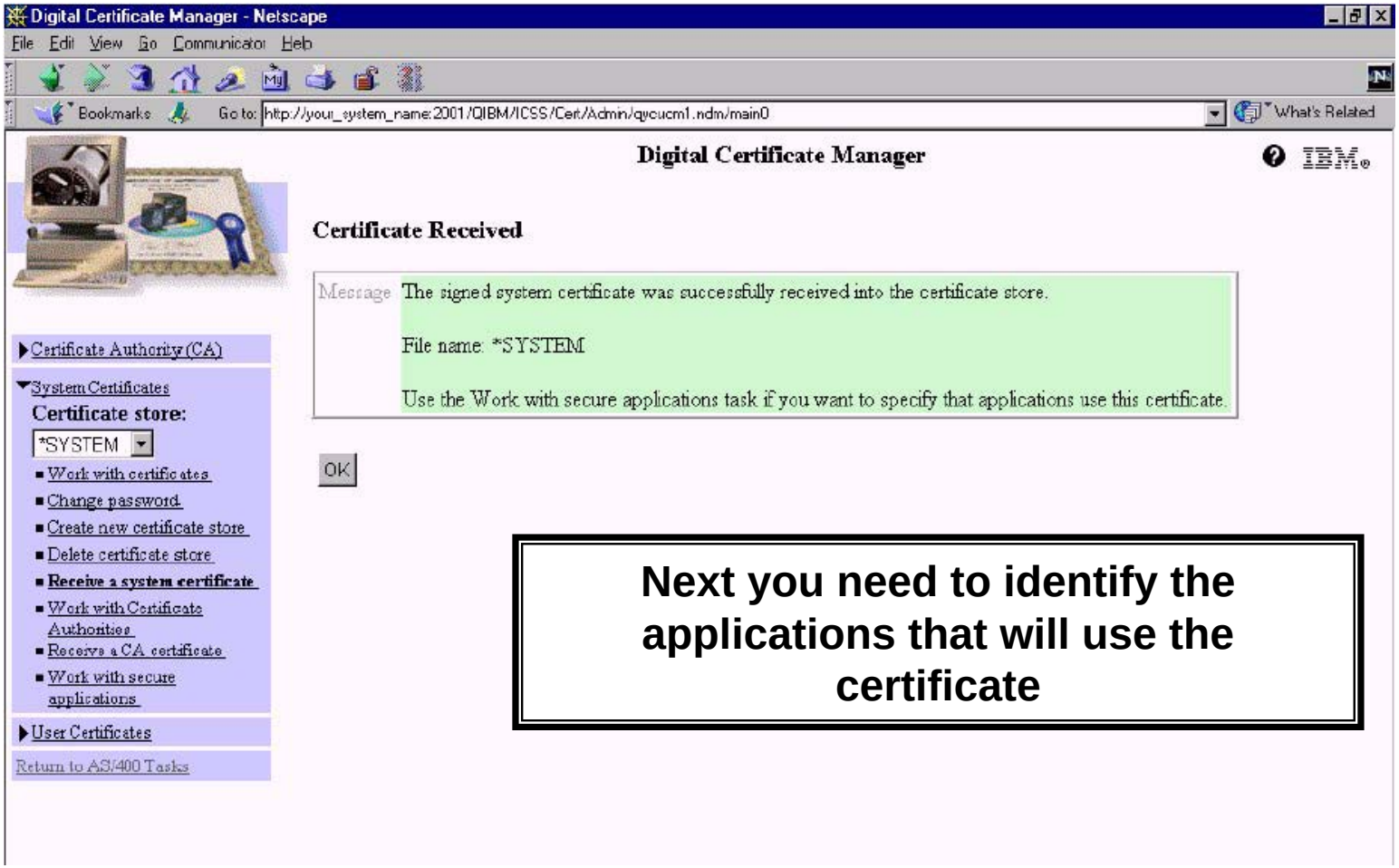
And COPY it, then paste it into an editor like Notepad and save it to a text file on the IFS

(you will also want to save a copy in another secure location)

Receive Certificate from Issuer


Digital Certificate Manager - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location: http://your.system.name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
What's Related
Digital Certificate Manager
IBM
Receive a System Certificate
Use this form to receive a system certificate into a certificate store after the certificate has been signed by a Certificate Authority. Before using this form, you must copy the signed certificate into a file which you specify below.
Certificate store: *SYSTEM
Signed certificate path and file name: /import/vericert.txt (required)
OK Cancel
Certificate Authority (CA)
System Certificates
Certificate store:
*SYSTEM
Work with certificates
Change password
Create new certificate store
Delete certificate store
Receive a system certificate
Work with Certificate Authorities
Receive a CA certificate
Work with secure applications
User Certificates
Return to AS/400 Tasks
Import the file you saved on the IFS

Receive Certificate from Issuer



Next you need to identify the applications that will use the certificate

Work with Certificates

- Manage Certificates
  - View certificate
  - Renew certificate
  - Import certificate
  - Export certificate
  - Delete certificate
  - Validate certificate
  - Assign certificate
  - Set CA status
  - Update CRL location assignment
  - Assign a user certificate

- Renew Certificate
  - make sure you have a reminder on your calendar!
- Validate Certificate
  - certificate is not expired
  - not listed in a Certificate Revocation List (CRL) as revoked
  - CA certificate for the issuing CA in the current certificate store
  - CA certificate is enabled and marked as trusted
- Import Certificate
  - from another 400 or from Internet CA
- Export Certificate
  - Only for another 400 (Bummer!)
  - Windows Server has Certificate Authority for working with certificates in Windows environment

View Certificate

Bookmarks Location: http://ca.system.name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0 What's Related

Digital Certificate Manager IBM

- Certificate Authority (CA)
- System Certificates

Certificate store: *SYSTEM

- **Work with certificates**
- Change password
- Create new certificate store
- Delete certificate store
- Receive a system certificate
- Work with Certificate Authorities
- Receive a CA certificate
- Work with secure applications

- User Certificates

Return to AS/400 Tasks

Subject:

Common name	www.yourserver.com
Organization unit	ITSO Raleigh
Organization name	IBM
Locality or city	Cary
State or province	North Carolina
Zip or postal code	
Country	US

Issuer:

Common name	
Organization unit	For VeriSign authorized testing only. No assurances (C)VS1997 www.verisign.com/repository/TestCPS Incorp. By Ref. Liab. LTD.
Organization name	VeriSign, Inc
Locality or city	
State or province	
Zip or postal code	
Country	

Associated key label: VeriSignServerCertificateTrial

Key length	2048
Private key	Yes
Trusted	Yes

Document: Done

Renew Certificate

Select a Certificate Store

Expand All | Collapse All

- Fast Path
- Create Certificate
- Create New Certificate Store
- Install Local CA Certificate on Your PC
- Manage Certificates
  - View certificate
  - Renew certificate

Digital Certificate Manager

IBM

Renew Certificate

Certificate type: Server or client
Certificate store: *SYSTEM
Default certificate label: Alliance website

Select a certificate, then select a button to perform an action on the certificate.

	Certificate	Common name
◉	Alliance website	ASPWEB.ALLIANCESYS.COM
○	Alliance ASPWEB	ASPWEB.ALLIANCESYS.COM

View | Renew | Cancel

Renew Certificate

Select a Certificate Store

Expand All | Collapse All

- Fast Path
- Create Certificate
- Create New Certificate Store
- Install Local CA Certificate on Your PC

Digital Certificate Manager

IBM

Select a Certificate Authority (CA)

Certificate type: Server or client

Certificate store: *SYSTEM

Certificate label: Alliance ASPWEB

Select the type of Certificate Authority (CA) that will sign this certificate.

- (•) Local Certificate Authority (CA)
- ( ) VeriSign or other Internet Certificate Authority (CA)

Continue | Cancel

Renew Certificate

This screen for LOCAL Certificate Authority renewal only

Digital Certificate Manager

Renew Certificate

Certificate type: Server or client
Certificate store: *SYSTEM
Original certificate label: Alliance ASPWEB

Use this form to renew the certificate. Please provide any missing information.

New certificate label: (required)
Key size: 1024 (bits)

Certificate Information

Common name: ASPWEB.ALLIANCESYS.COM (required)
Organization unit:
Organization name: Alliance Systems & Programming (required)
Locality or city:
State or province: Missouri (required:minimum of 3 characters)
Country or region: US (required)

Certificate Label must be Unique – I have started putting the expiration date in it

Subject Alternative Name

Note: Certificate extensions are not necessary for Secure Sockets Layer (SSL), but are recommended for Virtual Private Network (VPN).

IP version 4 address:
Fully qualified domain name: (host_name.domain_name)
E-mail address: (user_name@domain_name)

Continue Cancel

Alliance Systems & Programming

Renew Certificate

Digital Certificate Manager

Renew Certificate

Certificate type: Server or client
Certificate store: *SYSTEM
Certificate label: Alliance ASPWEB

This screen for Internet Certificate Authority renewal only

Create a new public-private key pair for this certificate?

- ○ **Yes** - Create a new key pair for this certificate.
- ◉ **No** - Import the renewed signed certificate from an existing file.

Continue Cancel

Yes – creates a new request
No – import a new certificate from the CA

Renew Certificate

Digital Certificate Manager IBM

Certificate Renewed Successfully

Message Your certificate was renewed and placed in the certificate store listed below.

Certificate type: Server or client
Certificate store: *SYSTEM
Certificate label: ASPWEB.ALLIANCESYS.COM exp 9-2005

Select which applications will use this certificate:

WARNING: WHEN YOU ASSIGN A CERTIFICATE TO A CLIENT APPLICATION AND A SERVER REQUESTS CLIENT AUTHENTICATION, THEN THE SERVER AUTHENTICATES ALL USERS OF THE APPLICATION BASED ON THAT CERTIFICATE. CONSEQUENTLY, THE SERVER DOES NOT AUTHENTICATE USERS ON AN INDIVIDUAL BASIS. TO ENSURE THAT THE SERVER AUTHENTICATES EACH USER OF A CLIENT APPLICATION INDIVIDUALLY OUTSIDE THE SSL PROTOCOL, DO NOT ASSIGN A CERTIFICATE TO THE CLIENT APPLICATION.

Select All | Clear All

	Application	Type	Assigned certificate
☐	OS/400 TCP Central Server	Server	Alliance website
☐	OS/400 TCP Database Server	Server	Alliance website
☐	OS/400 TCP Data Queue Server	Server	Alliance website
☐	OS/400 TCP Network Print Server	Server	Alliance website
☐	OS/400 TCP Remote Command Server	Server	Alliance website
☐	OS/400 TCP Signon Server	Server	Alliance website
☐	Directory Services server	Server	Alliance website
☐	Directory Services publishing	Client	Alliance ASPWEB

Remember to assign the renewed certificate to all the applications that used to use the old one!

- Manage Applications
  - View application definition
  - Update certificate assignment
  - Define CA trust list
  - Add application
  - Remove application
  - Update application definition
  - Validate application

Manage Applications

- Update Certificate Assignment
  - Make sure all your applications that will use SSL have a valid certificate assigned!
- Validate Application
  - certificate is assigned for the application
  - ensures that assigned certificate is valid
  - if the application is configured to use a Certificate Authority (CA) trust list, that trust list contains at least one CA certificate
  - CA certificates in the application CA trust list are valid
  -
- View Application Definition and Add Application
  - Can define your OWN applications & configure SSL

Define CA trust list

Digital Certificate Manager IBM

Define CA Trust List

Application type: Server
Application ID: QIBM_GLD_DIRSRV_SERVER
Application description: Directory Services server

Trust All | Trust None

Note: The Certificate Authorities (CAs) defined in the CA trust list for the application are checked. If you wish to change the trust list, click on the check box and select OK.

Trusted	Certificate Authority (CA)		
☑	Verisign Class 3 trusted root	View	Validate
☑	Entrust	View	Validate
☑	LOCAL_CERTIFICATE_AUTHORITY(2)	View	Validate
☑	Verisign class 3 intermediate ca	View	Validate
☑	Verisign Public Private Class 3 CA	View	Validate
☑	Integrion Certification Authority Root	View	Validate
☑	IBM World Registry Certification Authority	View	Validate
☑	Thawte Personal Premium CA	View	Validate
☑	Thawte Personal Freemail CA	View	Validate

Must define trusted CAs for EACH APPLICATION

Remember: application must be enabled for SSL before it will show up in the list!

Certificate Revocation List Location

Digital Certificate Manager

IBM

Add CRL Location

The Certificate Revocation List (CRL) location is the LDAP server where the CRL is stored. Use this form to define the location of the CRL.

Select a Certificate Store

Expand All | Collapse All

- Fast Path
- Create Certificate
- Create New Certificate Store
- Install Local CA Certificate on Your PC
- Manage Certificates
- Manage Applications
- Manage Certificate Store
  - Set default certificate
  - Change password
  - Delete certificate store
- Manage CRL Locations
  - View CRL location
  - **Add CRL location**
  - Update CRL location
  - Remove a CRL location
- Manage PKIX Request Location

Return to iSeries Tasks

Secure Connection

CRL Location Name:

LDAP Server Information:	
LDAP Server:	
Use Secure Sockets Layer (SSL):	○ Yes ◉ No
Port number:	

Connection Information:	
Login distinguished name (DN):	
Password:	

Note: To use an anonymous session, leave the login distinguished name (DN) and password blank.

OK | Cancel

LDAP server can provide a list of revoked certificates

Public Key Infrastructure (PKIX) Request Location

- PKIX Certificate Authorities require proof of identity from certificate requester through a Registration Authority (RA) before issuing certificate
- Configure a URL for a PKIX CA
- DCM provides PKIX CA as option for obtaining signed certificates
- Lotus(R) Domino(TM) provides a PKIX CA for public use

Enable SSL for HTTP Admin Server

1) Make sure that the ADMIN server is running.
2) Click the **Manage** tab …then Click the **All HTTP Servers** subtab.
3) Select **ADMIN** from the **Server** list.
4) Select **Include /QIBM/UserData/HTTPA/admin/conf/admin-cust.conf** from the **Server area** list.
5) Expand **Tools** and Select **Edit Configuration File**.
6) Enter the following information into the configuration file or remove the "#" symbol to uncomment these lines:

```
LoadModule ibm_ssl_module /QSYS.LIB/QHTTPSVR.LIB/QZSRVSSL.SRVPGM
Listen 2001
Listen 2010
SetEnv HTTPS_PORT 2010
<VirtualHost *:2010>
    SSLEnable
    SSLAppName QIBM_HTTP_SERVER_ADMIN
</VirtualHost>
```

7) Click **OK**.

Enable SSL for HTTP Admin Server

IBM Web Administration for iSeries

Setup | Manage | Advanced | Related Links

WebSphere IBM

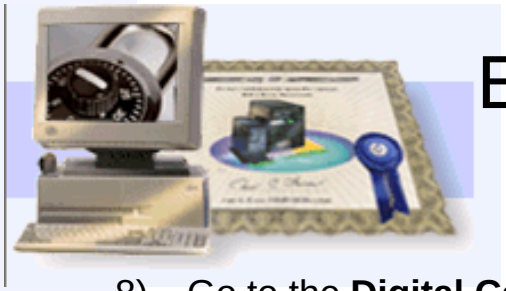
All Servers | HTTP Servers | Application Servers | ASF Tomcat Servers

Running Server: ADMIN - Apache Server area: Include /QIBM/UserData/HTTPA/admin/conf/admin-cust.c

- Common Tasks and Wizards
  - Create HTTP Server
  - Create Application Server
  - Migrate Original to Apache
- HTTP Tasks and Wizards
  - Add a Directory to the Web
  - LDAP Configuration
  - Servlet and JSP Enablement
- Server Properties
  - General Server Configuration
  - Container Management
  - Virtual Hosts
  - URL Mapping
  - Request Processing
  - HTTP Responses
  - Content Settings
  - Directory Handling

```
# Customer additions to the admin configuration
LoadModule ibm_ssl_module
/QSYS.LIB/QHTTPSVR.LIB/QZSRVSSL.SRVPGM
Listen 2001
Listen 2010
SetEnv HTTPS_PORT 2010
<VirtualHost *:2010>
    SSLEnable
    SSLAppName QIBM_HTTP_SERVER_ADMIN
</VirtualHost>
```

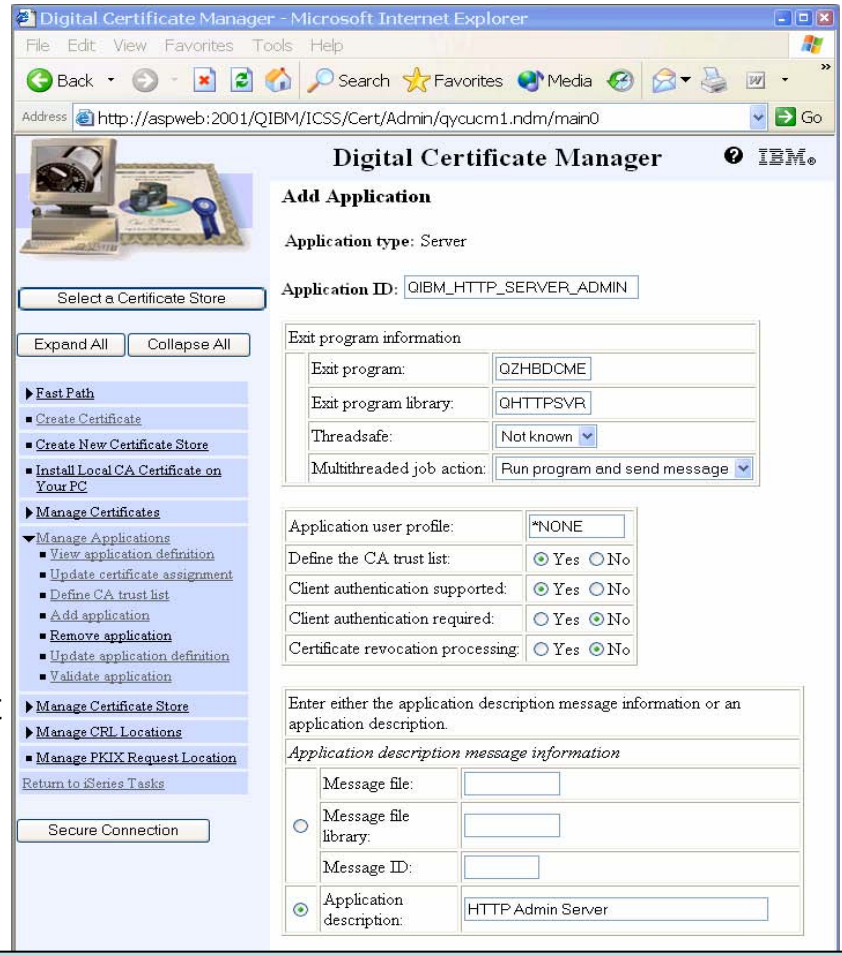
OK Apply Cancel



Enable SSL for HTTP Admin Server

(continued)

8) Go to the **Digital Certificate Manager**.
9) Click **Select a Certificate Store**.
10) Select ***SYSTEM**, then enter a password in the **Certificate store password** field on the next screen.
11) Expand **Manage Applications** and Select **Update certificate assignment**.
12) On the application type screen, select **Server**.
13) Select **QIBM_HTTP_SERVER_ADMIN** application name. (If it doesn't show up in the list, you may need to manually ADD the Application to the list using the parameters shown here, then come back to step 11 Update Certificate Assignment... If you END and restart the admin server to make it show up,… GOTCHA!!! the admin server will fail to start because it doesn't have a certificate assigned!! Catch-22!)



If you're stuck with an admin config file that won't start, you can get to it on a green screen with the command WRKLNK '/qibm/userdata/httpa/admin/conf'
Use option 2 to edit admin-cust.conf and put a # in the first position of the SSLENABLE and SSLAPPNAME lines to comment them out. Then save the file and STRTCPSVR *HTTP HTTPSVR(*ADMIN)

Enable SSL for HTTP Admin Server (continued)

14) Click **Update Certificate Assignment**.
15) Select the appropriate certificate.
16) Click **Assign New Certificate** to assign the certificate to the application name selected in the previous step.
17) If you had to manually add the application, next select **Define CA Trust List,** select **Server,** then select the server application you added **(QIBM_HTTP_SERVER_ADMIN)** and click **DEFINE CA TRUST LIST.** On the next screen click the **Trust All** button, then click **OK**.
18) Restart the ADMIN server
    - ENDTCPSVR *HTTP HTTPSVR(*ADMIN)
    - STRTCPSVR *HTTP HTTPSVR(*ADMIN)
19) Restart your Web browser.

To use the ADMIN server, type **http://[iSeries_hostname]:2001** for a non-secure connection or **https://[iSeries_hostname]:2010** for a secure connection.

Note: If you have trouble getting the secure connection working, check the ADMIN error log file located in the (**\QIBM\UserData\HTTPA\admin\logs** directory for information.

iSeries Server Applications that Support SSL

- iSeries Access
  - dataqueue
  - database
  - file server
  - network printer
  - Remote command
  - management central
  - signon
- DRDA & DDM (database access)
- FTP (file transfer)
- Telnet (terminal access)
- HTTP (original & Apache)
- Host on Demand
- Host Access Transform Server (HATS) & HATSLE
- Websphere Application Server
- Domino
- LDAP (directory services)
- EIM (Enterprise Identity Mapping)
- Applications written with:
  - Java Developer Kit or IBM Toolbox for Java
  - iSeries Access for Windows APIs
  - Global Secure Toolkit (GSKit)
  - SSL_iSeries Native APIs

Applications that support SSL: iSeries Access

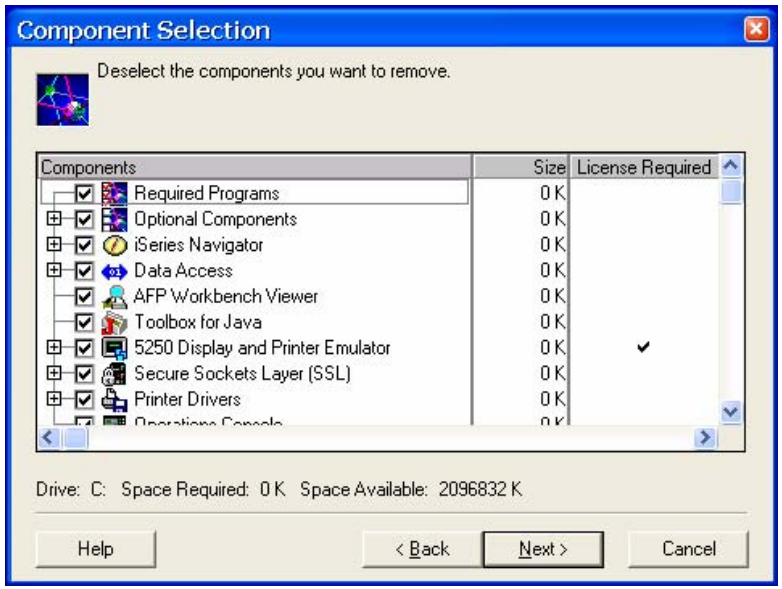
1) Authorize the appropriate user profile to the Client Encryption products.

WRKAUT OBJ('/QIBM/ProdData/CA400/EXPRESS/SSL/SSL40

or... use iSeries Navigator to edit permissions of SSLxx under Integrated File System

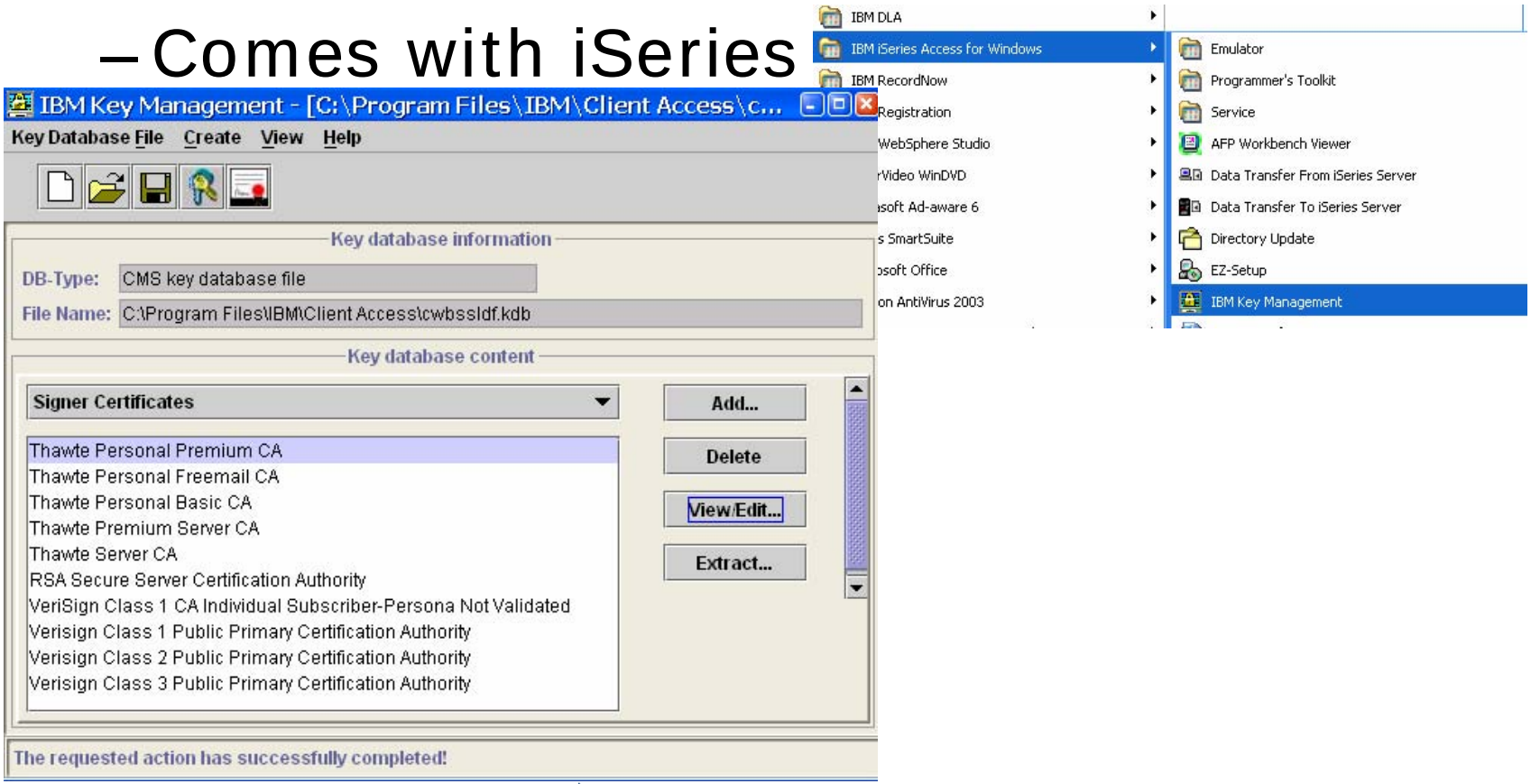
2) Install the SSL component of iSeries Access

- Use Selective Setup…


Component Selection
Deselect the components you want to remove.
Components
Size
License Required
Required Programs 0 K
Optional Components 0 K
iSeries Navigator 0 K
Data Access 0 K
AFP Workbench Viewer 0 K
Toolbox for Java 0 K
5250 Display and Printer Emulator 0 K
Secure Sockets Layer (SSL) 0 K
Printer Drivers 0 K
Drive: C: Space Required: 0 K Space Available: 2096832 K
Help
< Back
Next >
Cancel

Applications that support SSL: iSeries Access (continued)

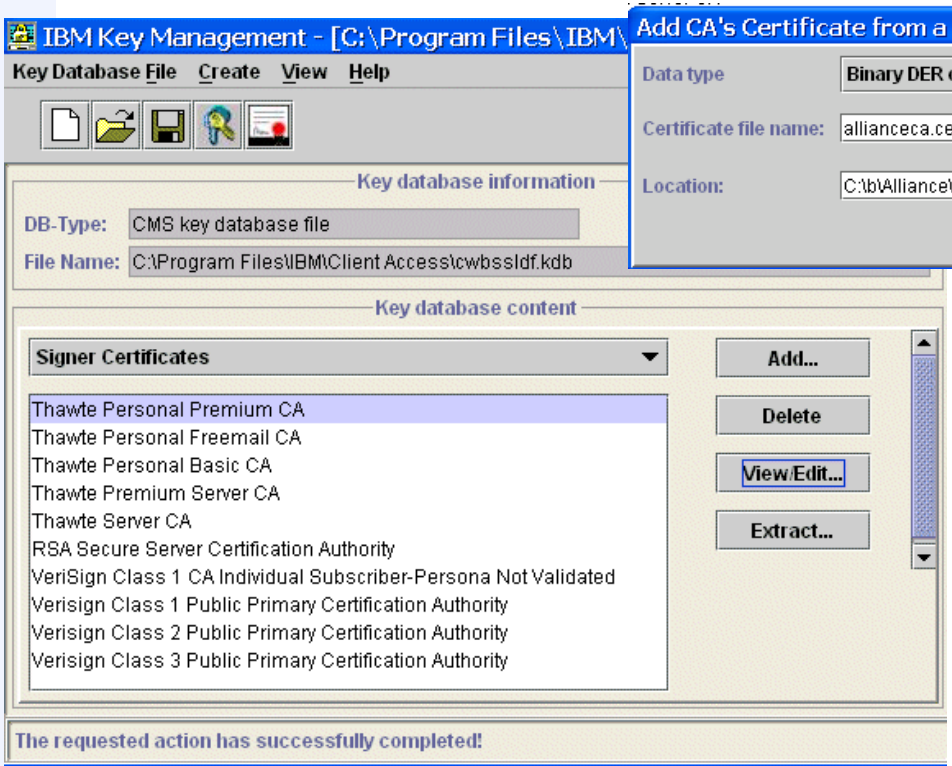
- IBM Key Management Utility
  - Comes with iSeries

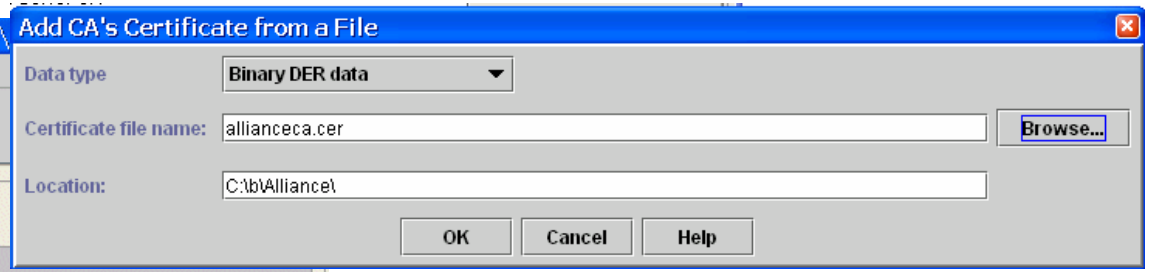


Applications that support SSL: iSeries Access (continued)

3) Add CA Cert using IBM Key Management Utility

- **Open iSeries Access key database file: cwbssldf.kdb**


IBM Key Management - [C:\Program Files\IBM\
Key Database File Create View Help
Key database information
DB-Type: CMS key database file
File Name: C:\Program Files\IBM\Client Access\cwbssldf.kdb
Key database content
Signer Certificates
Thawte Personal Premium CA
Thawte Personal Freemail CA
Thawte Personal Basic CA
Thawte Premium Server CA
Thawte Server CA
RSA Secure Server Certification Authority
VeriSign Class 1 CA Individual Subscriber-Persona Not Validated
Verisign Class 1 Public Primary Certification Authority
Verisign Class 2 Public Primary Certification Authority
Verisign Class 3 Public Primary Certification Authority
Add...
Delete
View/Edit...
Extract...
The requested action has successfully completed!

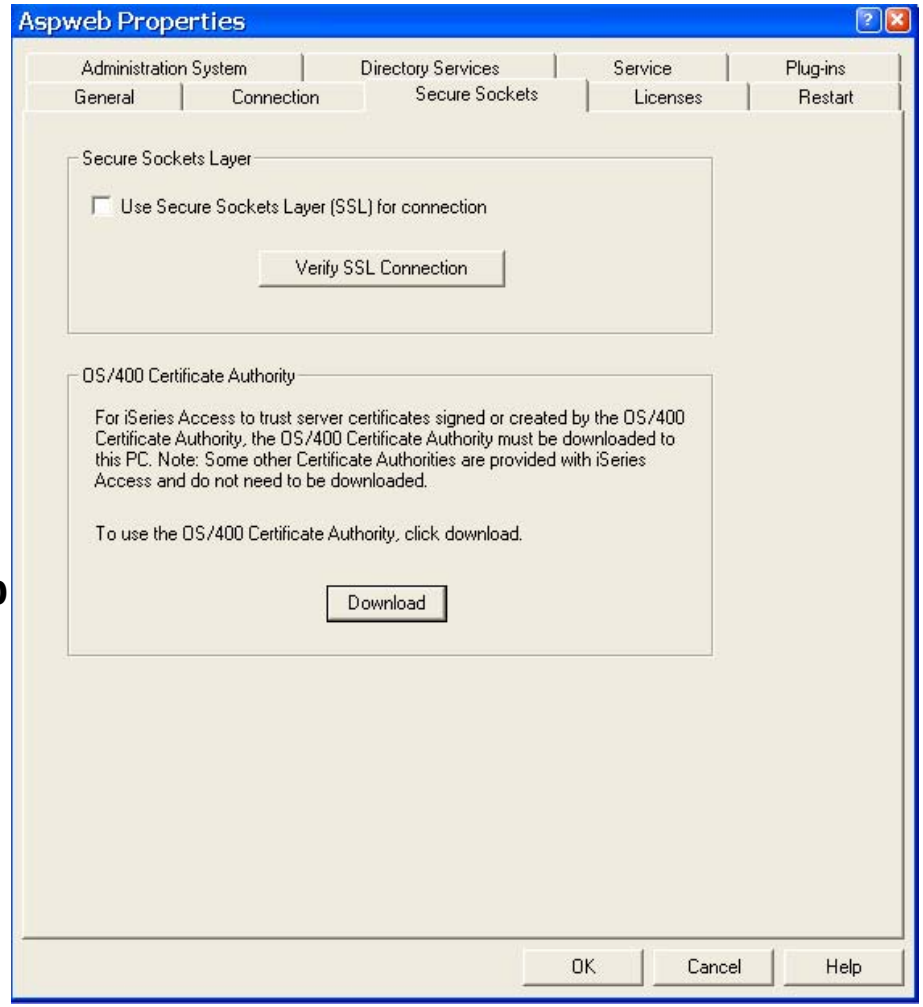


Alliance Systems & Programming

Applications that support SSL: iSeries Access

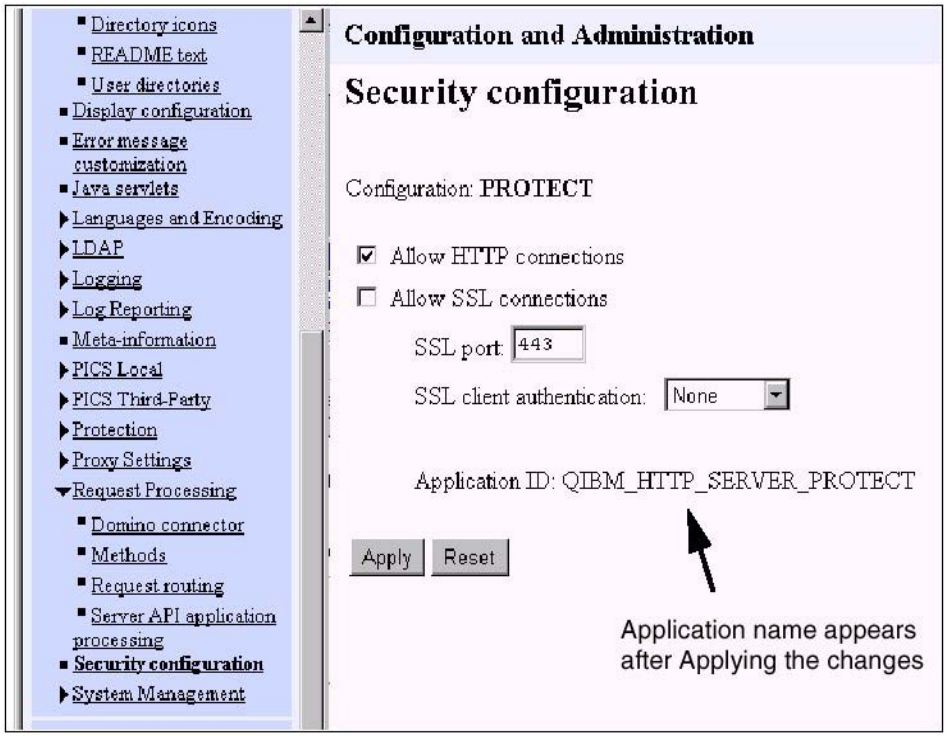
3) **Use Download utility to add CA cert to iSeries Access key database**

4) **Activate SSL for the iSeries Navigator client:**
   - **In iSeries Navigator, expand My Connections.**
   - **Right-click the system, and select Properties.**
   - **Click the Secure Sockets tab and select Use Secure Sockets Layer (SSL) for connection.**
   - **Exit iSeries Navigator and restart it.**


Aspweb Properties
Administration System
Directory Services
Service
Plug-ins
General
Connection
Secure Sockets
Licenses
Restart
Secure Sockets Layer
Use Secure Sockets Layer (SSL) for connection
Verify SSL Connection
OS/400 Certificate Authority
For iSeries Access to trust server certificates signed or created by the OS/400 Certificate Authority, the OS/400 Certificate Authority must be downloaded to this PC. Note: Some other Certificate Authorities are provided with iSeries Access and do not need to be downloaded.
To use the OS/400 Certificate Authority, click download.
Download
OK
Cancel
Help

Applications that support SSL: Original IBM HTTP server

1. Enable SSL in the HTTP server configuration



2. Assign the CA and Server certificate to the web server instance

Applications that support SSL: Apache HTTP Server

1) Set up a name-based virtual host

- Click the **Manage** tab, then Click the **HTTP Servers** subtab.
- Select your HTTP Server (powered by Apache) from the **Server** list.
- Select **Global configuration** from the **Server area** list.
- Expand **Server Properties** and Click **Virtual Hosts**, then Click the **Name-based** tab in the form.
- Click **Add** under the **Named virtual hosts** table.
- Enter an IP address in the **IP address** columnEnter a port number in the **Port** column. Example: 443
- Specify a port number to be used for SSL – default is 443
- Click **Add** under the **Virtual host containers** table in the **Named host** column. **Note:** This is a table within the **Named virtual hosts** table in the **Named host** column.
- Enter the fully qualified server hostname for the virtual host in the **Server name** column.
- **Note:** Make sure the server hostname you enter is fully qualified and associated with the IP address you selected in the iSeries TCP/IP host table
- Enter a document root for the virtual host index file or welcome file in the **Document root** column.
- Click **Continue, then** Click **OK**

Applications that support SSL: Apache HTTP Server (continued)

2) Set up Listen directive for virtual host

- Expand **Server Properties,** Click **General Server Configuration**, then Click the **General Settings** tab
- Click **Add** under the **Server IP addresses and ports to listen** on table.
- Select the IP address you entered for the virtual host in the **IP address** column.
- Enter the port number you entered for the virtual host in the **Port** column.
- Click **Continue,** then Click **OK**.

3) Set up the virtual host directories

- Select the virtual host from the **Server area** list.
- Expand **HTTP Tasks and Wizards,** Click **Add a Directory to the Web**, then Click **Next**.
- Select **Static web pages and files** and Click **Next**.
- Enter a directory name for the virtual host in the **Name** field. Click **Next**.
- Enter an alias for the virtual host in the **Alias** field. Example: /earnings/
- Click **Next**, then Click **Finish**.

The document root and directory for the virtual host has been created.

Applications that support SSL: Apache HTTP Server

4) Set up password protection via authentication

- Select the directory under the virtual host from the **Sever area** list.
- Expand **Server Properties,** Click **Security**, then Click the **Authentication** tab in the form.
- Select **Use OS/400® profile of client** under **User authentication method** for 400 native security
- Enter **iSeries Signon** in the **Authentication name or realm** field.
- Select **Default server profile** from the **OS/400 user profile to process requests** list under **Related information**. When selected, the value **%%SERVER%%** will be placed in the field.
- Click **Apply**, then Click the **Control Access** tab in the form.
- Click **All authenticated users (valid user name and password)** under **Control access based on who is making the request**, then Click **OK**.

5) Enable SSL for the virtual host

- Select the virtual host from the **Sever area** list. Example: Virtual Host *:443
- Expand **Server Properties**, then Click **Security**.
- Click the **SSL with Certificate Authentication** tab in the form.
- Select **Enable SSL** under **SSL**.
- Select **QIBM_HTTP_SERVER_[server_name]** from the **Server certificate application name** list. **Note:** Remember the name of the server. You will need to select it again in the Digital Certificate Manager.
- Select **Do not request client certificate for connection** under **Client certificates when establishing the connection** then Click **OK**.

Applications that support SSL: Apache HTTP Server

6) **Associate system certificate with HTTP Server (powered by Apache)**
   - Go to **Digital Certificate Manager** (http://yourserver:2001)
   - Click **Select a Certificate Store**, Select ***SYSTEM**, then Click **Continue**.
   - Enter a password in the Certificate store password field and Click **Continue**.
   - Click **Manage Applications**, Select **Update certificate assignment**, then Click **Continue**.
   - Select **Server** and Click **Continue**.
   - Select the appropriate application name and Click **Update Certificate Assignment**.
   - Select the appropriate certificate.
   - Click **Assign New Certificate**. This assigns the certificate to the application name selected in the previous step.
7) **Restart your HTTP Server (powered by Apache)**
   - Go to **HTTP Administration** and Click the **Manage** tab.
   - Click the **HTTP Servers** subtab.
   - Select your HTTP Server from the Server list.
   - Click the **Stop** icon if the server is running.
   - Click the **Start** icon.
8) **Test your HTTP Server (powered by Apache)**
   - Start a new Web browser.
   - Enter **https://yourserver:port** in the location or URL field.

Applications that support SSL: FTP

- **Enable SSL for the iSeries FTP server by:**
  - In iSeries Navigator, expand **the iSeries server** --> **Network** --> **Servers** --> **TCP/IP**.
  - Right-click **FTP**.
  - Select **Properties**, then Select the **General** tab.
  - Choose **Secure only** for SSL support
    Select this to allow only SSL sessions with the FTP server. Connections may be made to the non-secure FTP port, but the FTP client must negotiate an SSL session before the user is allowed to log in.
- **Enable SSL for the iSeries FTP Client Control Connection by:**
  - On the **STRTCPFTP** (FTP) command, specify **SECCNN** (***SSL)**
  - Within your FTP client session, use the **SECOPEN** subcommand
- **Enable SSL for the iSeries FTP Data Connection**
  - For the **STRTCPFTP** (FTP) command, enter **DTAPROT** (***PRIVATE)**
  - When you have a secure control connection, you can use the **SECDATA** subcommand to change the data connection protection level.

Applications that support SSL: Telnet Server

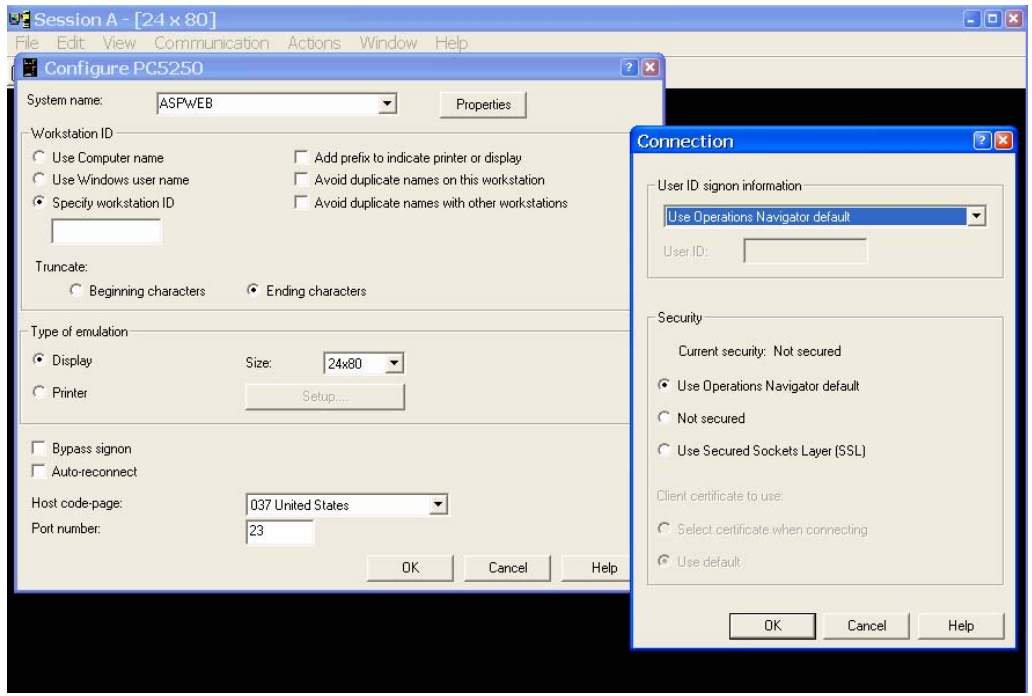
- **Remove any port restrictions**
  - Using iSeries Navigator, expand iSeries server --> Network.
  - Right-click TCP/IP Configuration and select Properties.
  - Click the Port Restrictions tab to see a list of port restriction settings.
  - Select the port restriction that you want to remove and click Remove, then click OK.
- **Enable SSL for Telnet**
  - Expand **My iSeries server** --> **Network** --> **Servers** --> **TCP/IP**.
  - Right-click **Telnet,** Select **Properties,** Select the **General** tab.
  - Choose one of these options for SSL support:
    - **Secure only**
      Select this to allow only SSL sessions with the Telnet server.
    - **Non-secure only**
      Select this to prohibit secure sessions with the Telnet server. Attempts to connect to an SSL port will not connect.
    - **Both secure and non-secure**
      Allows both secure and non-secure sessions with the Telnet server.
- **Configure the Telnet server to require certificates for client authentication** by selected YES to require client authenitication on DCM Application Definition for Telnet server application

Applications that support SSL: Telnet Client (continued)

- **Enable iSeries Access Client for SSL**
  - Open iSeries Navigator.
  - Right-click the name of your system, Select **Properties**.
  - Select the **Secure Sockets** tab. **Note:** This tab will not appear unless you have completed a selective install of iSeries Client Encryption (128-bit), 5722-CE3.
  - Click **Download** to download the CA certificate into the key database.
  - Enter your key database password (default is ca400)

- **Configure telnet session to use SSL and port 992**

This is all that is required to encrypt the session and validate the server certificate. If you want to also validate the user, you must use User Certificates



Alliance Systems & Programming

User Certificates

- **Used to authenticate user to a particular server**
  - **additional security**
  - **replace userid and password security**
  - **digital signature**

NOTE: The only way to create client user certificates using the AS/400 DCM is for the user to come to the DCM using a browser. The user has to enter the AS/400 system user name and password, and then request a certificate. The user profile must exist in advance. There is no way to create a certificate on behalf of another entity, nor to modify the creation of the certificate by using an exit program or something similar. When the certificate has been created, it is automatically associated with the user name that was given.

Applications that support SSL: Telnet Client User Certificates

- **Obtain a user certificate**
  - Start DCM (http://yourserver:2001)
  - In the left-hand navigation frame, select **Create Certificate** to display a list of tasks.
  - From the task list, select **User Certificate** and click **Continue**.
  - Complete the **User Certificate** form. Only those fields marked "Required" need to be completed. Click **Continue**.
  - Depending on the browser you use, you will be asked to generate a certificate that will be loaded into your browser. Follow the directions provided by the browser.
  - When the **Create User Certificate** page reloads, click **Install Certificate**. This will install the certificate in the browser.
  - Export the certificate to your PC. You must store the certificate in a password-protected file.
- **Enable iSeries Access to present certificate**
  - Start the **IBM Key Management Utility**
  - You will be prompted for your key database password. Unless you have previously changed the password from the default, enter ca400. A confirmation message displays. Click **OK**.
  - From the pull-down menu, select **Personal certificates**.
  - Click **Import**.
  - In the **Import key** display, enter the file name and path for the certificate. Click **OK**.
  - Enter the password for the protected file. This is the same password that you specified when you create a user certificate in DCM. Click **OK**. When the certificate has been successfully added to your personal certificates in IBM Key Management, you can use PC5250 emulator or any other Telnet application.

Signing Certificates

- Digitally sign objects to verify
  - Integrity of the object's contents
  - Object’s source of origin
- Use DCM to:
  - Issue signing certificates
  - Sign Objects
    - Can also use Management Central as of V5R2
  - Verify signatures on objects

Working with Certificates in Browsers

Adding certificate authority to browser

prompted when new certifying authority

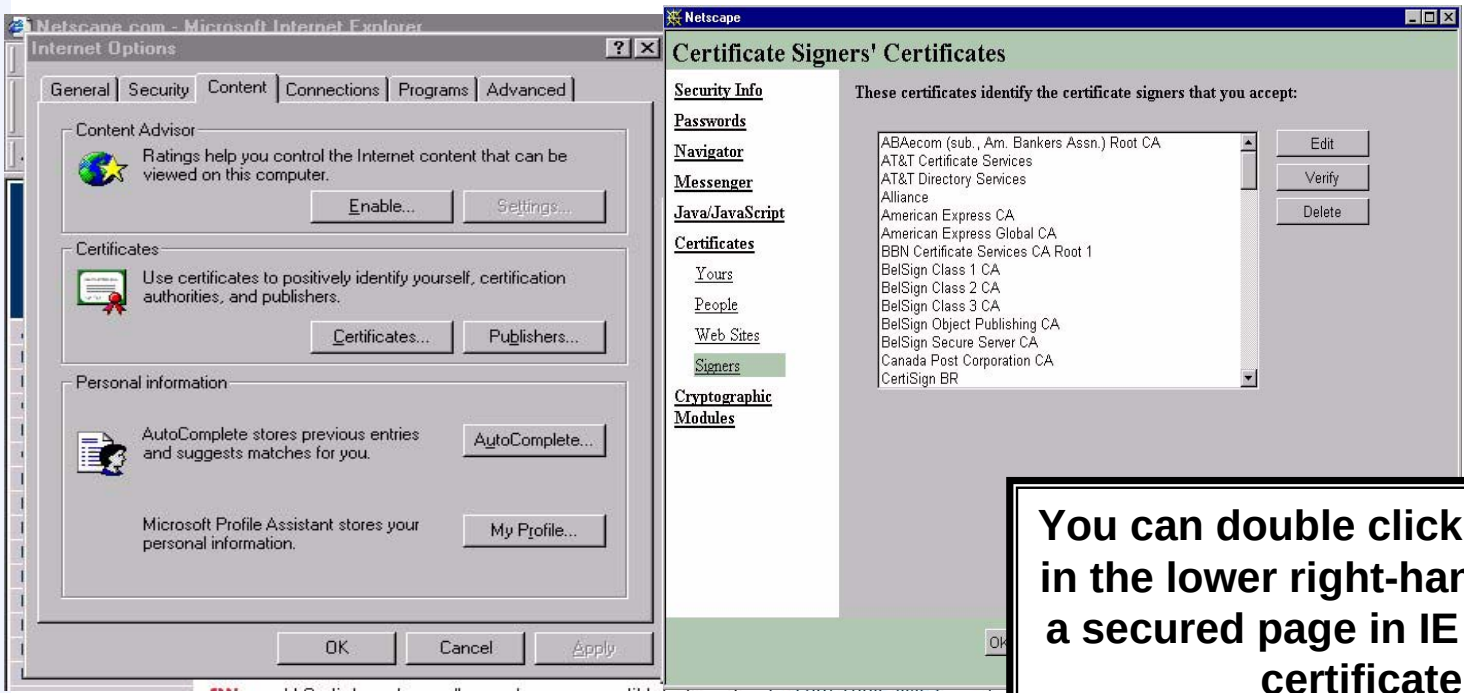
or server certificate received

Internet Explorer:

tools...internet options...content

Netscape Navigaor

Communicator...tools...security info



You can double click on the lock in the lower right-hand corner of a secured page in IE to view the certificate!

Alliance Systems & Programming

Importing a Certificate to Internet Explorer

Access the Certificate Import wizard from the view certificate window

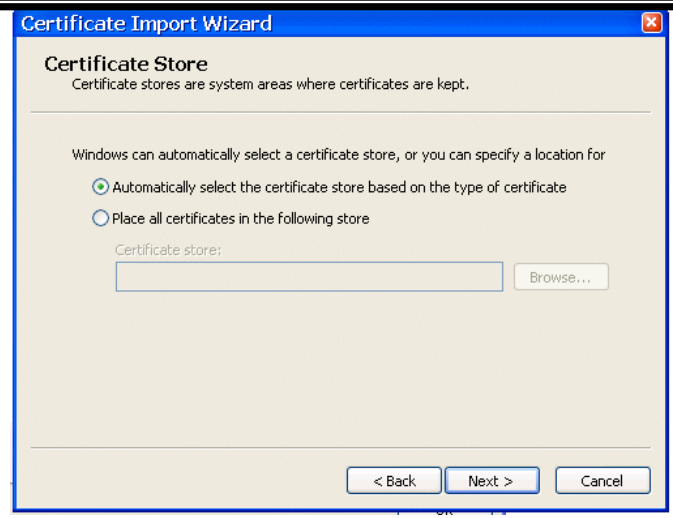
1)

Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
The security certificate has expired or is not yet valid.
The name on the security certificate is invalid or does not match the name of the site
Do you want to proceed?
Yes
No
View Certificate

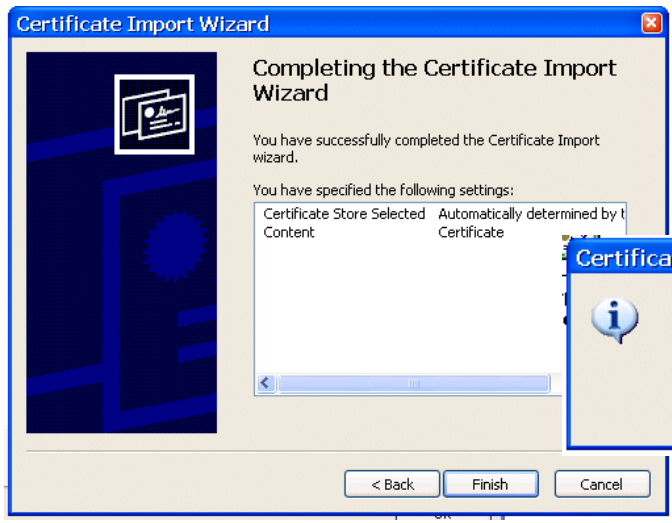
2)

Certificate Import Wizard
Welcome to the Certificate Import Wizard
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
To continue, click Next.
< Back
Next >
Cancel

3)


Certificate Import Wizard
Certificate Store
Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for
Automatically select the certificate store based on the type of certificate
Place all certificates in the following store
Certificate store:
Browse...
< Back
Next >
Cancel

4)



5)

Alliance Systems & Programming

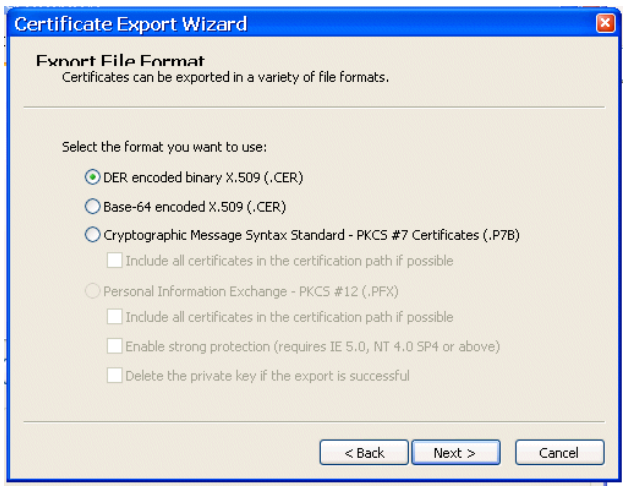
Exporting Certificate with Internet Explorer

Access the Certificate Export wizard from Tools… Internet Options…Content… Certificates

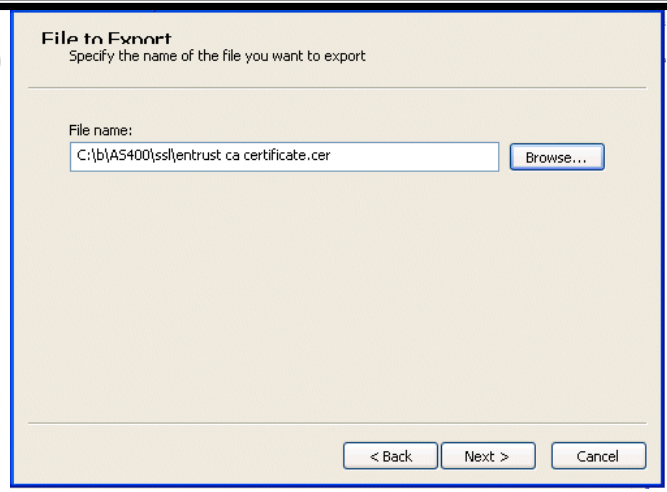
1)

Certificate Export Wizard
Welcome to the Certificate Export Wizard
This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
To continue, click Next.
< Back
Next >
Cancel

2)


Certificate Export Wizard
Export File Format
Certificates can be exported in a variety of file formats.
Select the format you want to use:
DER encoded binary X.509 (.CER)
Base-64 encoded X.509 (.CER)
Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
Include all certificates in the certification path if possible
Personal Information Exchange - PKCS #12 (.PFX)
Include all certificates in the certification path if possible
Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)
Delete the private key if the export is successful
< Back
Next >
Cancel

3)



4)

Certificate Export Wizard
Completing the Certificate Export Wizard
You have successfully completed the Certificate Export wizard.
You have specified the following settings:
File Name C:\b\A
Export Keys No
Include all certificates in the certification path No
File Format DER Er
< Back
Finish
Cancel

5)

Alliance Systems & Programming

Using SSL with Firewalls

Firewalls considerations: what ports needed?

- **Secure HTTP (https:) - port 443**
- **Secure FTP – 990**
- **Secure Telnet - port 992**
- **Secure DDM/DRDA - port 448**
- **Secure iseries access ports:**
  - **Management Central – 5566**
  - **Central server - 9470**
  - **Database server - 9471**
  - **Data Queue - 9472**
  - **File Server - 9473**
  - **Network Print - 9474**
  - **Remote Command - 9475**
  - **Signon Server – 9476**

AS/400 Internet Security: Developing a Digital Certificate Infrastructure (SG24-5659-00)